Cisco IOS CMTS Software Configuration Guide

First Published: 2007-01-01

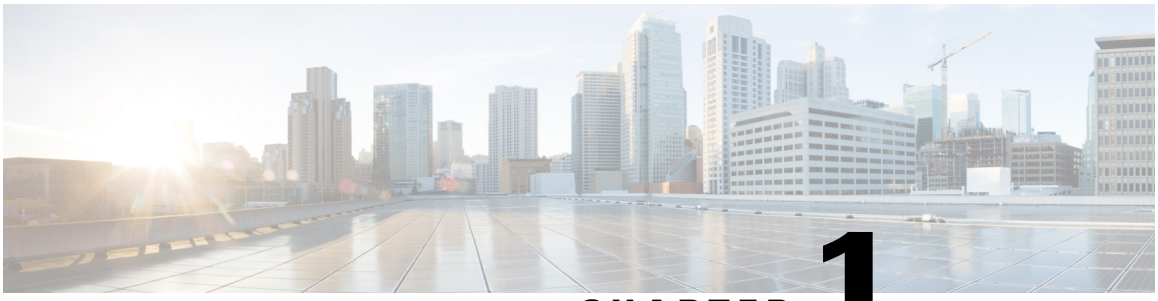
Last Modified: 2016-10-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

CMTS Router Basics



CHAPTER 1

Configuring the Cisco CMTS for the First Time

This chapter describes how to start up and configure the Cisco Cable Modem Termination System (CMTS) for the first time.

Note These sections provide minimal configuration instructions.

For detailed configuration information see the:

- Cisco IOS Configuration Fundamentals Configuration Guide, *Release 12.2* at http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html
- *Cisco IOS Configuration Fundamentals Command Reference* , *Release 12.2* at http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html

Note Be sure that you have appropriate addresses and values based on your network before you attempt to configure the router. Enter the **show version** command to display the release of Cisco software on your router.

Note Be sure to use **show** command a few seconds after configuration changes, or it might cause a crash.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring the Cisco CMTS

Complete these prerequisite steps before you power on and configure the Cisco CMTS:

- Ensure that your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified based on National Television Standards Committee (NTSC) or appropriate international cable plant recommendations. Ensure your plant meets all Data-over-Cable Service Interface Specifications (DOCSIS) downstream and upstream radio frequency (RF) requirements.
- Ensure that your Cisco CMTS is installed according to the instructions in the hardware installation guide available on Cisco.com.

- Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational (based on the supported services). This includes:
  - All routers
  - Servers (Dynamic Host Configuration Protocol (DHCP) servers, Trivial File Transfer Protocol (TFTP) servers, and time-of-day (ToD) servers)
  - Network management systems
  - Other configuration or billing systems
- Ensure that DHCP and DOCSIS configuration files have been created and pushed to appropriate servers so that each CM, when initialized, can:
  - Transmit a DHCP request
  - Receive an IP address
  - Obtain TFTP and ToD server addresses
  - Download a DOCSIS configuration file (or updated software image if using Cisco uBR924 cable access routers or Cisco uBR910 cable data service units (DSUs) in your network)
- Ensure that customer premises equipment (CPE)—CMs or set-top boxes (STBs), PCs, telephones, or facsimile machines—meet requirements for your network and service offerings.
- Be familiar with your channel plan to assign appropriate frequencies. Outline your strategies for setting up bundling, if applicable to your headend or distribution hub. As appropriate, obtain:
  - Passwords
  - IP addresses
  - Subnet masks
  - Device names

After these prerequisites are met, you are ready to configure the Cisco CMTS. This includes, at a minimum:

- Configuring a host name and password for the Cisco CMTS
- Configuring the CMTS to support IP over the cable plant and network backbone

Note If you plan to use service-class-based provisioning, the service classes must be configured at the CMTS before CMs attempt to make a connection.

Booting and Logging onto the Cisco CMTS

The Cisco CMTS is administered using the Cisco command interpreter, called the EXEC. You must boot and log in to the router before you can enter an EXEC command.

Step 1 Connect a terminal to the I/O controller console port of the Cisco CMTS and establish a terminal session. You can open a Terminal application (Hyper Terminal) on a PC as follows:

- Connect using: Direct to Com 1
- Set bits per second: 9600
- Set data bits: 8
- Set parity: none
- Set stop bit: 1
- Set flow control: none

Step 2 Power on the Cisco CMTS. Enter no to choose the normal operating mode of the router. The user EXEC prompt appears:

```
Would you like to enter the initial dialog?[yes]: no
Router>
```

Setting Password Protection on the Cisco CMTS

Note For security purposes, the EXEC has two levels of access to commands: user EXEC mode and privileged EXEC mode. The commands available at the user level are a subset of those available at the privileged level.

Tip Because many privileged-level EXEC commands are used to set operating parameters, password-protect these commands to prevent unauthorized use.

Note An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters. An enable password can contain any number of uppercase and lowercase alphanumeric characters. A number cannot be the first character. Spaces are valid password characters; for example, “two words” is a valid password. Leading spaces are ignored. Trailing spaces are recognized. Alphanumeric characters are recognized as uppercase or lowercase.

Passwords should be different for maximum security. If you enter the same password for both during the setup script, the system accepts it, but you receive a warning message indicating that you should enter a different password.

At the EXEC prompt, enter one of the following two commands to set password protection:

- **enable secret password—**a very secure encrypted password.
- **enable—**is a less secure and nonencrypted password.

To gain access to privileged-level commands, enter the desired password.

Recovering Lost Password on the Cisco CMTS

Complete the following steps to recover or replace a lost enable, enable secret, or console login password:

Step 1 Attach an ASCII terminal to the console port on your Cisco CMTS.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bits.

Step 3 If you can log in to the router as a nonprivileged user, enter the **show version** command to display the existing configuration register value. Note the value for later use. If you cannot log in to the router at all, continue with the next step.

Step 4 Press the Break key or send a Break from the console terminal.

- If Break is enabled, the router enters the ROM monitor, indicated by the ROM monitor prompt (rommon n>), where n is the number of the command line. Proceed to configuring the register.
- If Break is disabled, power cycle the router (turn the router off or unplug the power cord, and then restore power). Within 60 seconds of restoring the power to the router, press the Break key or send a Break. This action causes the router to enter the ROM monitor and display the ROM monitor prompt (rommon 1>).

Step 5 To set the configuration register on a Cisco CMTS, use the configuration register utility by entering the **confreg** command at the ROM monitor prompt as follows:

```
rommon 1> confreg
```

Answer yes to the *enable ignore system config info?* prompt and note the current configuration register settings.

Step 6 Initialize the router by entering the **reset** command as follows:

```
rommon 2> reset
```

The router initializes, the configuration register is set to 0x142, the router boots the system image from Flash memory and enters the System Configuration dialog (setup), as follows:

```
--- System Configuration Dialog --
```

Step 7 Enter no in response to the System Configuration dialog prompts until the following message appears:

```
Press RETURN to get started!
```

Step 8 Press Return. The user EXEC prompt appears as follows:

```
Router>
```

Step 9 Enter the **enable** command to enter privileged EXEC mode.

Step 10 Enter the **show startup-config** command to display the passwords in the configuration file as follows:

```
Router# show startup-config
```

Step 11 Scan the configuration file display looking for the passwords; the enable passwords are usually near the beginning of the file, and the console login or user EXEC password is near the end. The passwords displayed will look something like this:

```
enable secret 5 $1$ORPP$s9syZt4uKn3SnpuLDrhuei
enable password 23skiddoo
.
.
line con 0
 password onramp
```

Note The enable secret password is encrypted and cannot be recovered; it must be replaced. The enable and console passwords can be encrypted text or clear text.

Proceed to the next step to replace an enable secret, console login, or enable password. If there is no enable secret password, note the enable and console login passwords if they are not encrypted and proceed to set the configuration register to the original value.

Caution Do not perform the next step unless you have determined that you must change or replace the enable, enable secret, or console login passwords. Failure to follow the steps as presented here could cause your router configuration to be erased.

Step 12 (Optional) Enter the configure memory command to load the startup configuration file into running memory. This action allows you to modify or replace passwords in the configuration.

```
Router# configure memory
```

Step 13 Enter the **configure terminal** command for configuration mode:

```
Router# configure terminal
```

Step 14 To change all three passwords, enter the following commands:

```
Router(config)# enable secret newpassword1

Router(config)# enable password newpassword2
Router(config)# line con 0

Router(config)# password newpassword3
```

Change only the passwords necessary for your configuration. You can remove individual passwords by using the **no** form of the previous commands. For example, entering the **no enable secret** command removes the enable secret password.

Step 15 You must configure all interfaces to not be administratively shut down as follows:

```
Router(config)# interface fast ethernet 0/0/0

Router(config)# no shutdown
```

Enter the equivalent commands for all interfaces that were originally configured. If you omit this step, all interfaces are administratively shut down and unavailable when the router is restarted.

Step 16 Use the **config-register** command to set the configuration register to the original value noted earlier.

Step 17 Press Ctrl-Z or type **end** to exit configuration mode:

```
Router(config)# end
```

Caution Do not perform the next step unless you have changed or replaced a password. If you skipped changing or replacing the enable, enable secret, or console login passwords previously, then proceed now to reload. Failure to observe this sequence causes the system to erase your router configuration file.

Step 18 Enter the **copy running-config startup-config** command to save the new configuration to nonvolatile memory:

```
Router# copy running-config startup-config
```

Step 19 Enter the **reload** command to reboot the router:

```
Router# reload
```

Step 20 Log in to the router with the new or recovered passwords.

Configuring the Cisco CMTS Using AutoInstall

This section provides information about AutoInstall, a Cisco IOS software feature that allows you to configure a new router automatically and dynamically. The AutoInstall process involves connecting a new router to a network where an existing router is preconfigured, turning on the new router, and enabling it with a configuration file that is automatically downloaded from a TFTP server.

The AutoInstall process begins any time a Cisco IOS software-based device is turned on and a valid configuration file is not found in nonvolatile random-access memory (NVRAM).

The dynamic configuration of the new router occurs as follows:

1. The new router acquires its IP address. Depending on the interface connection between the two routers and/or access servers, the new router's IP address is dynamically resolved by either SLARP requests or BOOTP or RARP requests.
2. The new router resolves its name through network-confg, cisconet.cfg, or DNS.
3. The new router automatically requests and downloads its configuration file from a TFTP server.

If a host name is not resolved, the new router attempts to load router-confg or ciscortr.cfg.

Note If you wish to configure the device manually, you should connect directly to the console port and ensure that the router is not connected to the network via any of the interface ports before you turn on the router. Note that it may take several minutes for the device to determine that AutoInstall is not connected to the network.

Prerequisites for Using Autoinstall

- Routers must be attached physically to the network using one or more of the following interface types:
  - Ethernet
  - Token Ring
  - FDDI

- Serial with High-Level Data Link Control (HDLC) encapsulation
- Serial with Frame Relay encapsulation

Note HDLC is the default serial encapsulation. If the AutoInstall process fails over HDLC, the Cisco IOS software automatically configures Frame Relay encapsulation.

Note Of Token Ring interfaces, only those that set ring speed with physical jumpers support AutoInstall. AutoInstall does not work with Token Ring interfaces for which the ring speed must be set with software configuration commands. If the ring speed is not set, the interface is set to shutdown mode.

- A TCP/IP host on your network must be preconfigured to provide the required configuration files.
- The TCP/IP host can exist anywhere on the network as long as the following conditions are maintained:
  - The host must be on the LAN or WAN side of the router's line card connection to the WAN.
  - The User Datagram Protocol (UDP) broadcasts to and from the router.
  - The TCP/IP host is enabled.

This functionality is coordinated by your system administrator at the site where the TCP/IP host is located. You should not use AutoInstall unless the required files are available on the TCP/IP host.

Preparing for the AutoInstall Process

Complete the following steps to prepare your Cisco CMTS CMTS router for the AutoInstall process:

Step 1 Attach the appropriate synchronous serial cable to the synchronous serial interface 0 on the router.

Step 2 Turn the power switch on each power supply to the ON (|) position. This action turns on power to the router. The router loads the operating system image from Flash memory; this process can take several minutes. If the remote end of the WAN connection is connected and properly configured, the AutoInstall process begins.

Step 3 When the AutoInstall process is completed, use the copy running-config startup-config command to write the configuration data to the router's nonvolatile random-access memory (NVRAM):

```
Router# copy running-config startup-config
```

Completing this step saves the configuration settings that the AutoInstall process created to NVRAM. If you fail to do this, your configuration will be lost the next time you reload the router.

Step 4 Choose your preferred method to verify the required file configurations for the AutoInstall Facility:

Option	Description
Verify that the configuration file is on the TFTP server.	Complete this task first (required). Verify that a configuration file for the new router resides on a TFTP server. This file can contain the full or minimum-required configuration for the administrator to Telnet into the new router (for configuration using Autoinstall). **Note** In addition, complete one of the following two tasks.
Verify that a file named network-confg also resides on the TFTP server.	Complete this task, or the next. In this task, verify that the network-confg file on the TFTP server has an Internet Protocol (IP) host name entry for the new router. The TFTP server must be reachable from the new router.
Add IP-address-to-host name mapping to a DNS database file.	Complete this task, or the previous. In this task, add an IP address-to-host name mapping for the new router to a Domain Name System (DNS) database file on the TFTP server.

Step 5 If the existing router is to help install the new router automatically via an HDLC-encapsulated serial interface using Serial Line Address Resolution Protocol (SLARP), that interface must be configured with an IP address whose host portion has the value 1 or 2. (AutoInstall over Frame Relay does not have this address constraint.) Subnet masks of any size are supported.

Step 6 If the existing router is to help install the new router automatically using a Frame Relay-encapsulated serial interface, that interface must be configured with the following:

- An IP helper address pointing to the TFTP server. In the following example, 171.69.2.75 is the address of the TFTP server:
```
ip helper 171.69.2.75
```
- A Frame Relay map pointing back to the new router. In the following example, 172.21.177.100 is the IP address of the new router's serial interface, and 100 is the PVC identifier:
```
frame-relay map ip 172.21.177.100 100 dlci
```

Step 7 If the existing router is to help install the new router automatically via an Ethernet, Token Ring, or FDDI interface using BOOTP or Reverse Address Resolution Protocol (RARP), then a BOOTP or RARP server also must be set up to map the new router's Media Access Control (MAC) address to its IP address.

Step 8 IP helper addresses might need to be configured to forward the TFTP and DNS broadcast requests from the new router to the host that is providing those services.

Performing the AutoInstall Procedure

This procedure provides the steps to configure your Cisco uBR10012 router using AutoInstall.

Note For a detailed description of the processes involved with AutoInstall, refer to the "Using AutoInstall and Setup" chapter in the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 book on Cisco.com.

To dynamically configure a new router using AutoInstall, complete the following steps.

Note Steps 1, 2, and 3 are completed by the central administrator. Step 4 is completed by the person at the remote site.

Step 1 Modify the existing router's configuration to support the AutoInstall procedure.

Step 2 Set up the TFTP server to support the AutoInstall procedure.

Step 3 Set up the BOOTP or RARP server if needed. A BOOTP or RARP server is required for AutoInstall using an Ethernet, Token Ring, FDDI, or Frame Relay-encapsulated serial interface. With a Frame Relay-encapsulated serial interface, the existing router acts as the BOOTP server. A BOOTP or RARP server is not required for AutoInstall using an HDLC-encapsulated serial interface.

Step 4 Connect the new router to the network.

Configuring an Interface to Allow Use of AutoInstall

Using an HDLC-Encapsulated Serial Interface Connection

To set up AutoInstall via a serial line with HDLC encapsulation (the default), you must configure the existing router. Use the following commands, beginning in global configuration mode:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface serial** *interface-number*	Configures the serial interface that connects to the new router with HDLC encapsulation (the default), and enters interface configuration mode for the specified interface number.
Step 2	**ip address** *address mask*	Enters an IP address for the interface. The host portion of the address must have a value of 1 or 2. (AutoInstall over Frame Relay does not have this address constraint.)
Step 3	**ip helper-address** *address*	Configures a helper address for the serial interface to forward broadcasts associated with the TFTP, BOOTP, and DNS requests.
Step 4	**clock rate** *bps*	(Optional) Configures a DCE clock rate for the serial line, unless an external clock is being used. This step is needed only for DCE appliques.
Step 5	Ctrl-Z	Exits configuration mode.

	Command or Action	Purpose
Step 6	**copy running-config startup-config**	Saves the configuration file to your startup configuration. On most platforms, this step saves the configuration to NVRAM. On the Cisco7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable.

In the following example, the existing router's configuration file contains the commands needed to configure the router for AutoInstall on a serial line using HDLC encapsulation:

```
Router# more system:startup-config

. . .

interface serial 0

 ip address 172.31.10.1 255.255.255.0

 ip helper-address 172.31.20.5

. . .
```

Using an Ethernet, Token Ring, or FDDI Interface Connection

To set up AutoInstall using an Ethernet, Token Ring, or FDDI interface, you must modify the configuration of the existing router. Use the following commands, beginning in global configuration mode:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** {**ethernet** | **tokenring** | **fddi**} *interface-number*	Enters interface configuration mode for the specified LAN interface.
Step 2	**ip address** *address mask*	Specifies an IP address for the interface.
Step 3	**ip helper-address** *address*	(Optional) Configures a helper address to forward broadcasts associated with the TFTP, BOOTP, and DNS requests.
Step 4	Ctrl-Z	Exits configuration mode.
Step 5	**copy running-config startup-config**	Saves the configuration file to your startup configuration. On most platforms, this step saves the configuration to NVRAM. On the Cisco7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable.

Typically, the LAN interface and IP address are already configured on the existing router. You might need to configure an IP helper address if the TFTP server is not on the same network as the new router.

In the following example, the existing router's configuration file contains the commands needed to configure the router for AutoInstall on an Ethernet interface:

```
Router# more system:startup-config
. . .
interface Ethernet 0
ip address 172.31.10.1 255.255.255.0
ip helper-address 172.31.20.5
. . .
```

Using a Frame Relay-Encapsulated Serial Interface Connection

To set up AutoInstall via a serial line with Frame Relay encapsulation, you must configure the existing router. Use the following commands beginning in global configuration mode:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface serial 0**	Configures the serial interface that connects to the new router, and enters interface configuration mode.
Step 2	**encapsulation frame-relay**	Configures Frame Relay encapsulation on the interface that connects to the new router.
Step 3	**frame-relay map ip** *ip-address dlci* or **frame-relay interface-dlci** *dlci option* [**protocol ip** *ip-address*]	Creates a Frame Relay map pointing back to the new router. Or for point-to-point subinterfaces, assigns a data link connection identifier (DLCI) to the interface that connects to the new router, and provides the IP address of the serial port on the new router.
Step 4	**ip address** *address mask*	Specifies an IP address for the interface. This step sets the IP address of the existing router.
Step 5	**ip helper-address** *address*	Configures a helper address for the TFTP server.
Step 6	**clock rate** *bps*	(Optional) Configures a DCE clock rate for the serial line, unless an external clock is being used. This step is needed only for DCE appliques.
Step 7	Ctrl-Z	Exits configuration mode.
Step 8	**copy running-config startup-config**	Saves the configuration file to your startup configuration. **Note** On most platforms, this step saves the configuration to NVRAM. On the Cisco 7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable.

You must use a DTE interface on the new router because the network always provides the clock signal. In the following example, the existing router's configuration file contains the commands needed to configure the router for Frame Relay AutoInstall on a serial line:

```
Router# more system:startup-config
```

```
. . .
interface serial 0
ip address 172.31.20.20 255.255.255.0
encapsulation frame-relay
frame-relay map ip 172.31.10.1 255.255.255.0 48
ip helper-address 172.31.20.5
. . .
```

Setting Up the TFTP Server for Autoinstall

For AutoInstall to work correctly, the new router must be able to resolve its host name and then download a name-confg or a name.cfg file from a TFTP server. The new router can resolve its host name by using a network-confg or a cisconet.cfg file downloaded from a TFTP server or by using the DNS.

To set up a TFTP server to support AutoInstall, perform the following steps:

Step 1 Enable TFTP on a server. For information on this process, consult your host vendor's TFTP server documentation and RFCs 906 and 783.

Step 2 If you want to use a network-confg or cisconet.cfg file to resolve the new router's name, create the network-confg or cisconet.cfg file containing an IP address-to-host name mapping for the new router. Enter the ip host command into the TFTP config file, not into the router. The IP address must match the IP address that is to be dynamically obtained by the new router.
If you want to use DNS to resolve the new router's name, create an address-to-name mapping entry for the new router in the DNS database. The IP address must match the IP address that is to be dynamically obtained by the new router. For more information on this step, contact your DNS administrator or refer to RFCs 1101 and 1183

Step 3 Create the name-confg or name.cfg file, which should reside in the tftpboot directory on the TFTP server. The name part of name-confg or name.cfg filename must match the host name you assigned for the new router in the previous step. Enter configuration commands for the new router into this file.
The name-confg or the name.cfg file can contain either the new router's full configuration or a minimal configuration.

The minimal configuration file is a virtual terminal password and an enable password. It allows an administrator to Telnet into the new router to configure it. If you are using BOOTP or RARP to resolve the address of the new router, the minimal configuration file must also include the IP address to be obtained dynamically using BOOTP or RARP.

You can use the copy running-config tftp command to help you generate the configuration file that you later download during the AutoInstall process.

Note The existing router might need to forward TFTP requests and response packets if the TFTP server is not on the same network segment as the new router. When you modified the existing router's configuration, you specified an IP helper address for this purpose.

You can save a minimal configuration under a generic newrouter-confg file. Use the ip host command in the network-confg or cisconet.cfg file to specify newrouter as the host name with the address you will be dynamically resolving. The new router should then resolve its IP address, host name, and minimal configuration automatically.

Use Telnet to connect to the new router from the existing router and use the setup command facility to configure the rest of the interfaces. For example, the line in the network-confg or cisconet.cfg file could be similar to the following:

```
ip host newrouter 131.108.170.1
```

The following host configuration file contains the minimal set of commands needed for AutoInstall using SLARP or BOOTP:

```
enable-password letmein

!

line vty 0

password letmein

!

end
```

The preceding example shows a minimal configuration for connecting from a router one hop away. From this configuration, use the setup facility to configure the rest of the interfaces. If the router is more than one hop away, you also must include routing information in the minimal configuration.

The following minimal network configuration file maps the new router's IP address, 131.108.10.2, to the host name newrouter. The new router's address was learned via SLARP and is based on the existing router's IP address of 131.108.10.1.

```
ip host newrouter 131.108.10.2
```

Setting Up the BOOTP or RARP Server for Autoinstall

If the new router is connected to the existing router using an Ethernet, Token Ring, or FDDI interface, you must configure a BOOTP or RARP server to map the new router's MAC address to its IP address. If the new router is connected to the existing router using a serial line with HDLC encapsulation, or if you are configuring AutoInstall over Frame Relay, the tasks in this section are not required.

To configure a BOOTP or RARP server, use one of the following:

Step 1 Refer to your host vendor's documentation and RFCs 951 and 1395. If BOOTP is to be used to resolve the new router's IP address, configure your BOOTP server.

Step 2 Refer to your host vendor's documentation and RFC 903. If RARP is to be used to resolve the new router's IP address, configure your RARP server.

Note If the RARP server is not on the same subnet as the new router, use the **ip rarp-server** command to configure the existing router to act as a RARP server.

The following host configuration file contains the minimum set of commands needed for AutoInstall using RARP. It includes the IP address that will be obtained dynamically via BOOTP or RARP during the AutoInstall process. When RARP is used, this extra information is needed to specify the proper netmask for the interface.

```
interface ethernet 0

ip address 131.108.10.2 255.255.255.0

enable-password letmein
```

```
!
line vty 0
password letmein
!
end
```

Connecting the New Router to the Network

Connect the new router to the network using either an HDLC-encapsulated or Frame Relay-encapsulated serial interface or an Ethernet, Token Ring, or FDDI interface. After the router successfully resolves its host name, newrouter sends a TFTP broadcast requesting the file name-confg or name.cfg. The router name must be in all lowercase, even if the true host name is not. The file is downloaded to the new router, where the configuration commands take effect immediately. If the configuration file is complete, the new router should be fully operational.

To save the complete configuration to NVRAM, use the following commands in privileged EXEC mode:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable password**	Enters privileged mode on the new router.
Step 2	**copy running-config startup-config**	Saves the information from the name-config file into your startup configuration. On most platforms, this step saves the configuration to NVRAM. **Note** Verify that the existing and new routers (or access servers) are connected before entering the **copy running-config startup-config** EXEC command to save configuration changes. Use the **ping** EXEC command to verify connectivity. If an incorrect configuration file is downloaded, the new router will load NVRAM configuration information before it can enter AutoInstall mode. If the configuration file is a minimal configuration file, the new router comes up, but with only one interface operational. Use the following commands to connect to the new router and configure it:
Step 3	**telnet existing**	Establishes a Telnet connection to the existing router.
Step 4	**telnet newrouter**	From the existing router, establishes a Telnet connection to the new router.
Step 5	**enable password**	Enters privileged EXEC mode.
Step 6	**setup**	Enters setup mode to configure the new router.

Configuring the Cisco CMTS Router Using the Setup Facility

The Cisco CMTS Setup facility (also called the System Configuration dialog) is a useful and efficient tool for configuring your CMTS. The Cable Interface Setup Facility is an alternative mechanism to enable or configure Cisco CMTS parameters. The Setup facility supports automated configuration of upstream parameters.

In earlier releases, upstream ports were put in a default shut-down state after the Setup facility was run. You had to use the CLI to configure a fixed frequency or create a spectrum group, assign an interface to it, and enable each upstream port on a cable interface line card. The Setup facility now supports configuring and enabling upstream parameters.

The Setup facility supports the following functions so that cable interfaces and cable interface line cards are fully operational after initial setup:

- Cable-specific commands
- Upstream frequency definition

For each cable interface, the following information is mandatory:

```
Per upstream:
               cable upstream n frequency f
               no cable upstream n shutdown
```

Options include definition of the following information:

- DHCP server address.
- Options are also provided to set downstream frequency for the upconverter per interface.

If you do not plan to use AutoInstall, do not connect the router's WAN or LAN cable to the channel service unit (CSU) and data service unit (DSU). If the WAN or LAN cable is connected to the CSU and DSU and the router does not have a configuration stored in NVRAM, the router attempts to run AutoInstall at startup.

Tip The router might take several minutes to determine that AutoInstall is not set up to a remote TCP/IP host.

When the router determines that AutoInstall is not configured, it defaults to the Setup facility. If the LAN or WAN cable is not connected, the router boots from Flash memory and automatically runs the Setup facility.

Note You can run the Setup facility when the enable prompt (#) is displayed, by entering the setup command in privileged EXEC mode.

Configuring Global Parameters with the Setup Facility

Step 1 When you first start the program, configure the global parameters to control system-wide settings:
Connect a console terminal to the console port on the I/O controller, and then boot the router from Flash memory.

After booting, the following information appears after about 30 seconds. When you see this information, you have successfully booted your router:

```
       Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph
```

```
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-IK1S-M), Version 12.1(10)EC
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 24-Nov-01 12:59 by yiyan
Image text-base: 0x60008950, data-base: 0x61478000
Compliance with U.S. Export Laws and Regulations - Encryption
This product performs encryption and is regulated for export
by the U.S. Government.
This product is not authorized for use by persons located
outside the United States and Canada that do not have prior
approval from Cisco Systems, Inc. or the U.S. Government.
This product may not be exported outside the U.S. and Canada
either by physical or electronic means without PRIOR approval
of Cisco Systems, Inc. or the U.S. Government.
Persons outside the U.S. and Canada may not re-export, resell,
or transfer this product by either physical or electronic means
without  prior approval of Cisco Systems, Inc. or the U.S.
Government.
Cisco uBR7246VXR (NPE300) processor (revision D) with 253952K/40960K bytes
```

```
of memory.

Processor board ID SAB0433019F

R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

6 slot VXR midplane, Version 2.0

Last reset from power-on

Bridging software.

X.25 software, Version 3.0.0.

2 FastEthernet/IEEE 802.3 interface(s)

4 Serial network interface(s)

4 Cable Modem network interface(s)

125K bytes of non-volatile configuration memory.

125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).

4096K bytes of Flash internal SIMM (Sector size 256K).

cable submgmt default active

Press RETURN to get started!
```

Note The first two sections of the configuration script, the banner and the installed hardware, appear only at initial system startup. On subsequent uses of the **Setup facility**, the script begins with the following prompt.

```
     --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity

for management of the system, extended setup will ask you

to configure each interface on the system
```

Step 2 When asked if you want to continue with the System Configuration dialog and enter basic management setup (displays the current interface summary), enter **yes** or press **Return**:

```
Continue with configuration dialog? [yes/no]: yes
.
.
.
Would you like to enter basic management setup? [yes/no]: yes
```

Step 3 The interface summary appears, showing the state of configured and unconfigured interfaces.
Choose which protocols to support on your interfaces. For IP-only installations, you can accept the default values for most of the questions. A typical configuration using IP follows and continues:

```
Configuring global parameters:

  Enter host name [Router]: router
```

Step 4 Enter the **enable secret password**, the **enable password**, and the **virtual terminal password**.
The enable secret password is a one-way cryptographic secret password used instead of the enable password when it exists. The enable password is used when there is no enable secret password and when using older software and some boot images.

```
Enter enable secret: ******
Enter enable password: ******
Enter virtual terminal password: ******
```

Step 5 The Simple Network Management Protocol (SNMP) is the most widely supported open standard for network management. SNMP provides a means to access and set configuration and run-time parameters of routers and communication servers. SNMP also defines a set of functions that can be used to monitor and control network elements.
Enter yes to accept SNMP management; enter no to refuse it:

```
Configure SNMP Network Management? [no]:

    Community string [public]:
```

Step 6 In all cases, you will use IP routing. When you are using IP routing, select an interior routing protocol. You can specify one of only two interior routing protocols to operate on your system using the Setup facility, either In terior Gateway Routing Protocol (IGRP) or Routing Information Protocol (RIP).
To configure IP routing, enter yes (the default) or press Return, and then select an interior routing protocol:

```
  Configure IP? [yes]:

    Configure IGRP routing? [yes]:

      Your IGRP autonomous system number [1]: 15
```

Step 7 Configure your line card interface parameters. The following example shows how an 8-port Ethernet line card is installed in line card slot 3. The Setup facility determines the status of all interfaces.

To configure each active interface port for IP, enter yes (the default) or press Return . For all inactive ports, the default is no. You can press Return to accept the default.

```
Configuring interface Ethernet 1/0:

  Is this interface in use? [yes]:

  Configure IP on this interface? [yes]:

    IP address for this interface [19.2.22.4]:

    Number of bits in subnet field [8]:

    Class A network is 19.0.0.0, 8 subnet bits; mask is /16

Configuring interface Ethernet1/1:

  Is this interface in use? [no]:

Configuring interface Ethernet1/2:

Is this interface in use? [no]:

Configuring interface Ethernet1/3:

  Is this interface in use? [no]:

Configuring interface Ethernet1/4:

  Is this interface in use? [no]:

Configuring interface Ethernet1/5:

  Is this interface in use? [no]:

Configuring interface Ethernet1/6:

  Is this interface in use? [no]:

Configuring interface Ethernet1/7:

  Is this interface in use? [no]:
```

Step 8 Configure your cable interface. The following example shows a Cisco CMTS with cable interface. The Setup facility, for the most part, determines the status of all interfaces.
To configure each active interface port, enter yes (the default) or press Return . For all inactive ports, the default is no. You can press Return to accept the default.

```
Configuring interface cable 5/0:

  Is this interface in use? [yes]:
```

```
  Configure this interface? [yes]:
  IP address for this interface [19.2.22.5]:
  Number of bits in subnet field [8]:
  Class A network is 19.0.0.0, 8 subnet bits; mask is /16
Configuring interface cable 1/1:
  Is this interface in use? [yes]:
  Configure this interface? [yes]:
  IP address for this interface [19.2.22.6]:
  Number of bits in subnet field [8]:
  Class A network is 19.0.0.0, 8 subnet bits; mask is /16
```

The configuration program displays the newly created command interface script:

```
The following command script was created:
hostname router
enable secret 5 $1$f0fc$A38P/KN/9yD3sEKSt6hKQ/
enable password betty
line vty 0 4
password wilma
snmp-server community public
!
ip routing
!
interface cable 5/0
ip address 19.2.22.5 255.255.0.0
router igrp 15
network 19.0.0.0
!
```

```
end
```

Step 9 When asked if you want to use this configuration, enter yes or press Return.

```
Use this configuration? [yes/no]: yes
```

Step 10 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

Configuring Upstream Frequencies with the Setup Facility

Upstream parameters must be configured manually. After the Setup facility is run, upstream ports have a default state of "shutdown." You have two methods to configure upstream channel frequencies:

- Configure a fixed frequency between 5 to 42 MHz for North American channel plans, and enable the upstream port.
- Create a global spectrum group, assign the interface to it, and enable the upstream port.

The cable interface card receiver accepts time-division multiplexed burst transmissions from cable interfaces (or CMs in set-top boxes), which are DOCSIS-based. The upstream port becomes "up" when it is assigned an upstream frequency and is configured to be administratively up.

The upstream port is frequency-agile. The frequency can change while the interface is up and carrying traffic.

Configuring Individual Upstream Modulation Profiles

You can define individual modulation profiles. A modulation profile consists of a table of physical layer characteristics for the different types of upstream bursts such as initial maintenance, long grant, request data, request, short grant, and station maintenance.

Note Only qualified personnel should define upstream modulation profiles.

Complete these steps to activate upstream interfaces:

Step 1 After the Setup facility has initially configured noncable interfaces on the Cisco CMTS, enter the **enable** command and your password (privileged EXEC).

Step 2 Enter the **configure terminal** command to get into global configuration mode.

Step 3 In global configuration mode, configure modulation profiles and spectrum groups for your Cisco CMTS using the **cable modulation-profile** and **cable spectrum-group** commands.

Step 4 In cable interface configuration mode, configure various characteristics for the interface in question, using the **cable upstream** commands.

Configuring the Cisco CMTS Manually Using Configuration Mode

You can configure the Cisco CMTS manually if you prefer not to use the Setup facility or AutoInstall. Complete the following steps:

Step 1 Connect a console terminal to the console port on the I/O controller.

Step 2 When asked if you want to enter the initial dialog, answer no to go into the normal operating mode of the router:

```
Would you like to enter the initial dialog? [yes]: no
```

Step 3 After a few seconds, the user EXEC prompt (Router>) appears. Type **enable** to enter enable mode (configuration changes can be made only in enable mode):

```
Router> enable
```

The prompt changes to the enable mode (also called privileged EXEC) prompt:

```
Router#
```

Step 4 Enter the **configure terminal** command at the enable prompt to enter configuration mode from the terminal:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#
```

Note To see a list of the configuration commands available to you, enter ? at the prompt or type help while in configuration mode.

Step 5 At the Router(config)# prompt, enter the **interface** *type slot*/*port* command to enter the interface configuration mode:

```
Router(config)# interface cable slot/port
Router(config-if)#
```

Step 6 Set the downstream center frequency to reflect the digital carrier frequency of the downstream RF carrier (the channel) for the downstream port:

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

Note This command has no effect on the external upconverter. It is informational only.

Step 7 Activate the downstream port on the cable interface line card to support digital data transmission over the hybrid fiber-coaxial network:

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

Step 8 Enter the fixed center frequency in Hz for your downstream RF carrier and the port number:

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

Note Be sure not to select an upstream frequency that interferes with that used for any other upstream application in your cable plant.

Note Repeat this step for each upstream port on the cable interface line card.

Step 9 Activate the upstream port:

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

Note Repeat this step to activate each port used on your cable interface line card.

Step 10 Exit to return to the configuration mode.

```
Router(config-if)# exit
Router(config)#
```

Note

Step 11 Perform these steps on the other interfaces or type **exit** to return to enable mode.

```
Router(config)# exit
Router#

%SYS-5-CONFIG_I: Configured from console by console#
```

Step 12 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

Removing the Cable Interfaces

Removing the Wideband Cable Interface

To remove or delete a wideband cable interface, do the following:

Step 1 Reset the configuration of the interface back to its default values using the **default** command in global configuration mode.
On the Cisco uBR10012 router:

```
Router(config)# default interface wideband-Cable slot/{subslot | bay}/port:wideband-channel
```

On the Cisco uBR7200 series routers:

```
Router(config)# default interface wideband-Cable slot/port:wideband-channel
```

Step 2 Enter the wideband cable interface configuration mode.
On the Cisco uBR10012 router:

```
Router(config)# interface wideband-Cable slot/{subslot | bay}/port:wideband-channel
```

On the Cisco uBR7200 series routers:

```
Router(config)# interface wideband-Cable slot/port:wideband-channel
```

Step 3 Shut down the wideband cable interface.

```
Router(config-if)# shutdown
```

Step 4 Exit the wideband cable interface configuration mode.

```
Router(config-if)# exit
```

Step 5 Exit the global configuration mode.

```
Router(config)# exit
```

Removing the Integrated Cable Interface

To remove or delete an integrated cable interface, do the following:

Step 1 Reset the configuration of the interface back to its default values using the **default** command in global configuration mode.
On the Cisco uBR10012 router:

```
Router(config)# default interface Integrated-Cable slot/subslot/port:rf-channel
```

On the Cisco uBR7200 series routers:

```
Router(config)# default interface Integrated-Cable slot/port:rf-channel
```

Step 2 Enter the integrated cable interface configuration mode.
On the Cisco uBR10012 router:

```
Router(config)# interface Integrated-Cable slot/subslot/port:rf-channel
```

On the Cisco uBR7200 series routers:

```
Router(config)# interface Integrated-Cable slot/port:rf-channel
```

Step 3 Shut down the integrated cable interface.

```
Router(config-if)# shutdown
```

Step 4 Exit the integrated cable interface configuration mode.

```
Router(config-if)# exit
```

Step 5 Exit the global configuration mode.

```
Router(config)# exit
```

Removing the Modular Cable Interface

To remove or delete a modular cable interface, do the following:

Step 1 Reset the configuration of the interface back to its default values using the default command in global configuration mode.

```
Router(config)# default interface Modular-Cable slot/{subslot | bay}/port:interface-number
```

Step 2 Enter the modular cable interface configuration mode.

```
Router(config)# interface Modular-Cable slot/{subslot | bay}/port:interface-number
```

Step 3 Shut down the modular cable interface.

```
Router(config-if)# shutdown
```

Step 4 Exit the modular cable interface configuration mode.

```
Router(config-if)# exit
```

Step 5 Exit the global configuration mode.

```
Router(config)# exit
```

Configuring Interfaces with the Setup Facility

Configuring Ethernet Interfaces

Step 1 In the following example, the system is being configured for an Ethernet LAN using IP. Respond to the prompts as follows, using your own addresses and mask at the setup prompts:

Example:

```
Configuring interface parameters:
Configuring interface Ethernet0/0:
Is this interface in use? [no]: yes
Configure IP on this interface? [no]: yes
IP address for this interface: 1.1.1.10
Number of bits in subnet field [0]:
Class A network is 1.0.0.0, 0 subnet bits; mask is 255.0.0.0
```

Step 2 Do not enable Internetwork Package Exchange (IPX) on this interface; IPX is not supported on the Cisco uBR7200 series universal broadband router:

Example:

```
Configure IPX on this interface? [no]: no
```

Step 3 If additional Ethernet interfaces are available in your system, enter their configurations when you are prompted.

Step 4 Save the configuration to NVRAM:

Example:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

Configuring Synchronous Serial Interfaces

The synchronous serial interfaces are configured to allow connection to WANs through a CSU/DSU.

Complete the following steps to configure the serial ports:

Step 1 To configure serial port 0 enter yes:

Example:

```
Configuring interface Serial0/0:
Is this interface in use? [no]: yes
```

Step 2 Determine which protocols you want on the synchronous serial interface and enter the appropriate responses:

Example:

```
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 10.1.1.20
Number of bits in subnet field [0]:
Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
```

Step 3 If additional synchronous serial interfaces are available in your system, enter their configurations when you are prompted.

Step 4 Save the configuration to NVRAM:

Example:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

The following sample display includes a continuous listing of all interface configuration parameters selected for Ethernet and synchronous serial interfaces. These parameters are shown in the order in which they appear on your console terminal.

Tip Only one Ethernet and one synchronous serial interface are configured for this example.

```
Configuring interface parameters:

Configuring interface Ethernet0/0:
  Is this interface in use? [no]: yes

  Configure IP on this interface? [no]: yes

   IP address for this interface: 10.1.1.10

   Number of bits in subnet field [0]:
   Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
 Configure IPX on this interface? [no]:
 Configure AppleTalk on this interface? [no]: no
```

```
Configuring interface Serial0/0:
  Is this interface in use? [no]: yes

  Configure IP on this interface? [no]: yes

  Configure IP unnumbered on this interface? [no]:
    IP address for this interface: 10.1.1.20

    Number of bits in subnet field [0]:
    Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
  Configure IPX on this interface? [no]:
  Configure AppleTalk on this interface? [no]:

The following configuration command script was created:

hostname Router
enable secret 5 $1$u8z3$PMYY8em./8sszhzk78p/Y0
enable password wilma
line vty 0 4
password s
snmp-server community public
!
ip routing
no vines routing
no ipx routing
no appletalk routing
no apollo routing
no decnet routing
no xns routing
no clns routing
no bridge 1

! Turn off IPX to prevent network conflicts.
interface Ethernet0/0
no ipx network
interface Ethernet0/1
no ipx network
!
interface Ethernet0/0
ip address 1.1.1.10 255.0.0.0
no mop enabled
!
interface serial0/0
ip address 1.1.1.20 255.0.0.0
ip route-cache cbus
no keepalive
!
!
router igrp 15
network 1.0.0.0
!
end

Use this configuration? [yes/no]: yes

[OK]
Use the enabled mode `configure' command to modify this configuration.

Press RETURN to get started!
```

Your Cisco CMTS is now minimally configured and is ready to use. Use the **setup** command in provileged EXEC mode if you want to modify the parameters after the initial configuration. To perform more complex configurations, use the configure privileged EXEC command in global configuration mode.

Setup Facility Examples

In the following example, the upstream parameters for a cable interface line card in slot 5 are configured and enabled. Press Return to accept the default.

```
Do you want to configure Cable 5/0 interface? [no]: yes
Downstream setting frequency: 531000000
For cable upstream [0]
Shut down this upstream? [yes/no]: no
Frequency: 33808000
Would you like to configure the DHCP server? [yes/no]: yes
IP address for the DHCP server [X.X.X.X]: 10.0.0.2
Configure IP on this interface? [yes]:
IP address for this interface [10.20.133.65]:
Subnet mask for this interface [255.0.0.0]: 255.255.255.248
Class A network is 10.0.0.0, 29 subnet bits; mask is /29
In this example, the input above generates the following command interface script:
interface Cable 5/0
no shutdown
cable downstream frequency 531000000
no shutdown
cable downstream modulation 64qam
cable downstream annex B
cable downstream interleave-depth 32
no cable upstream 0 shutdown
cable upstream 0 frequency 33808000
cable helper-address 10.0.0.2
ip address 10.20.133.65 255.255.255.248
```

Note Cable modems or set-top boxes with integrated cable modems are brought online when the utility is run.

Note For Dynamic Host Configuration Protocol (DHCP)/time of day (TOD)/Trivial File Transfer Protocol (TFTP), a static route must exist to the host.

Configuring the Cable Interface with the Extended Setup Facility

The Setup facility creates an initial configuration. The basic management setup configures only enough connectivity for management of the system. The Extended Setup facility prompts you to configure each interface on the system.

To invoke the configuration facility, use the following command:

```
Router# setup
```

The following is the System Configuration dialog:

```
Continue with configuration dialog? [yes/no]: yes
```

MAC-Layer Addressing

The 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 unique to each port. The Cisco CMTS uses a specific method to assign and control the MAC-layer addresses for line cards.

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 line card and replace it with another identically configured one. If the new line card matches the line 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 Cisco CMTS midplane. Each address is reserved for a specific port and slot in the router regardless of whether a line card resides in that slot.

Note When hot swapping a line card with a different type of interface, you might have to reconfigure the interfaces. Refer to the hardware installation guide that ships with your CMTS or to the appropriate field-replaceable unit (FRU) document for more specific information regarding OIR.

The MAC addresses are assigned to the slots in sequence. This address scheme allows you to remove line cards and insert them into other Cisco CMTS 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 that the addresses stay with the memory device on which they are stored.

Identifying the Interfaces on a Line Card

The Cisco CMTS supports one downstream modulator and one upstream demodulator.

- The Cisco CMTS 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 downstream modulator has both an RF output, using the integrated upconverter, and an intermediate frequency (IF) output, which must be connected to an external upconverter.

Identifying CM Line Card Slots

On the Cisco CMTS, the cable interface line card is fixed and is always slot 1. To display information about a specific cable interface slot's downstream channel, use the **show interfaces cable** command with the CM 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 shows the display for upstream channel port 0 on a Cisco CMTS:

```
Router# sh int c 5/0/0
```

To display information about a specific cable interface slot's upstream channel, use the **show interfaces cable** command. Include these CM card parameters:

- Slot number
- Downstream port number

- Upstream port number

Use this format:
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 CMTS that is turned up:

```
Router# sh int c3/0/0 upstream
```

Configuring Global Parameters

Step 1 Access the host by responding to the following prompt:

```
Enter host name [cmts]:
```

Step 2 The **enable secret password** is used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.
Respond to this prompt:

```
Enter enable secret [Use current secret]: aa
```

Step 3 The **enable password** is used when you do not specify an **enable secret password**, with some older software versions, and some boot images.
Respond to this prompt:

```
Enter enable password [rHoz]: bb
```

Step 4 Use the virtual terminal password to protect access to the router over a network interface.
Respond to this prompt:

```
Enter virtual terminal password [cc]: cc
```

The following system information appears.

```
Configure SNMP Network Management? [no]:

Configure IP? [yes]:

Configure IGRP routing? [yes]:

Your IGRP autonomous system number [1]:

Configure CLNS? [no]:

Configuring interface parameters:

Do you want to configure FastEthernet0/0  interface? [yes]:
```

```
Use the 100 Base-TX (RJ-45) connector? [yes]:

Operate in full-duplex mode? [no]:

Configure IP on this interface? [yes]: no

Do you want to configure Ethernet1/0  interface? [yes]: n

Do you want to configure Cable5/0/0  interface? [yes]:

Downstream setting frequency  : 531000000

For cable upstream [0]

Shut down this upstream ? [yes/no]: no

Frequency  : 33808000

Would you like to configure the DHCP server ? [yes/no]: yes

IP address for the DHCP server

[X.X.X.X]: 10.0.0.2

Configure IP on this interface? [no]: yes

IP address for this interface: 10.20.133.65

Subnet mask for this interface [255.0.0.0] : 255.255.255.248

Class A network is 10.0.0.0, 29 subnet bits; mask is /29
```

The following configuration command script is created:

```
interface cable5/0/0

ip address 10.20.133.65 255.255.255.248

no ip mroute-cache

no keepalive

cable insertion-interval 500

cable downstream annex B

cable downstream modulation 64qam

cable downstream interleave-depth 32

cable downstream frequency 531000000
```

```
cable upstream 0 frequency 33808000

cable upstream 0 power-level 0

no cable upstream 0 shutdown

cable helper-address 10.0.0.2
```

Note For modems to acquire an IP address, they must have direct access to DHCP, TFTP, or ToD servers, or have a static route set.

Saving Your Configuration Settings

To store the configuration or changes to your startup configuration in NVRAM, enter the **copy running-config startup-config** command at the *Router#* prompt.

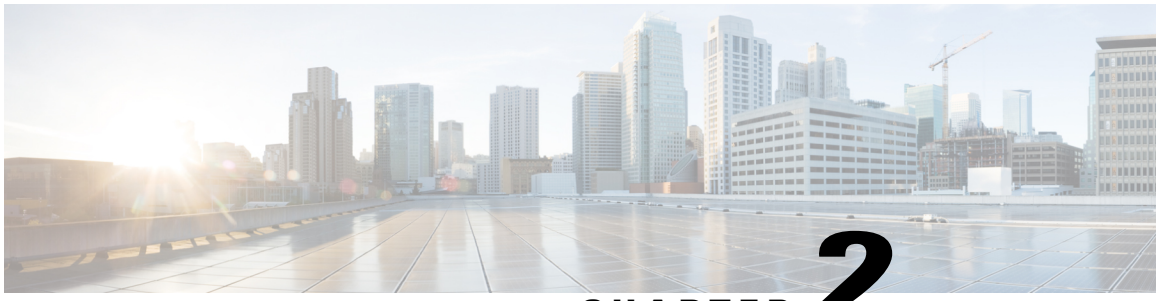
This command saves the configuration settings you set using configuration mode, the Setup facility, or AutoInstall.

Note If you do not save your settings, your configuration will be lost the next time you reload the router.

```
Router# copy running-config startup-config
```

Reviewing Your Settings and Configurations

- To view the current configuration of a Cisco CMTS, run the **show running-config** command at the command-line interface (CLI) prompt in EXEC mode or privileged EXEC mode.
- To review changes you make to the configuration, use the EXEC **show startup-config** command to display the information stored in NVRAM.



CHAPTER 2

Performing OIR of Cable Interface Line Cards on the Cisco CMTS

First Published: February 14, 2008

Last Modified: February 14, 2009

The Cisco uBR7200 series and Cisco uBR10012 universal broadband routers support online insertion and removal (OIR) of cable interface line cards, but have different requirements. The following sections describe this support for each of the platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

OIR of Cable Interface Line Cards on the Cisco uBR7200 Series Routers

Technically, the Cisco uBR7200 series universal broadband routers support true online insertion and removal (OIR), or hot swapping, of cable interface line cards only when exchanging cable interface line cards of the exact same type (for example, exchanging a Cisco uBR-MC28U card for another Cisco uBR-MC28U card). Under these conditions, no reload of the router is required.

Note When you OIR different types of cable interface line cards (for example, a Cisco uBR-MC16U card replaced by a Cisco uBR-MC16X card, or Cisco uBR-MC16U card replaced by a Cisco uBR-MC28U card), you not only might have to reconfigure the interfaces, we recommend that you reload the router.

For detailed OIR procedure information, see the product hardware installation guide available on Cisco.com.

Performing OIR of Cable Interface Line Cards on the Cisco uBR10012 Router

To perform an OIR of cable interface line cards on the Cisco uBR10012 router, do the following steps:

Step 1 From global configuration mode, enter the **cr10k card oir-compatibility** command for the cable interface line card that you want to OIR.

Example:
```
Router(config)# cr10k card 8/0 oir-compatibility
```
This command helps preserve the configuration and performs some internal synchronization to make sure that the OIR runs successfully.

Note The console log displays a new message appears whenever a line card type has been replaced. For example, if the MC520U-D in subslot 8/1 is replaced by an MC520S-D, the following message is displayed:

```
%UBR10K-6-COMPAT_NEW_CARD: The 5cable-mc520u-d in slot 8/1 has been replaced by a
5cable-mc520s-d
```
This message appears when an OIR operation involves two different types of MC520 line cards.

Caution The console log message does not appear for cards other than the MC520S/U/H. It also does not appear if the OIR operation involves identical MC520 card types. For instance, it will not appear if an MC520U is replaced by another MC520U. In such cases, you not only might have to reconfigure the interfaces, we recommend that you reload the router.

Step 2 Save the configuration to ensure the transition.

Example:
```
Router# copy running-config startup-config
```
Step 3 Turn the power off to the line card using the **cable power off** command for the slot that is being replaced.

Example:
```
Router# cable power off 8/0
Line Card 8/0 is POWERED OFF
This powers off the line card gracefully.
```
Step 4 Before removing the card, verify that the proper grounding instructions have been followed for the card.

Step 5 Remove the line card.

Step 6 Replace it with the new line card in the slot.

Step 7 Enter the **cable power on** command to power up the line card.

Example:
```
Router# cable power on 8/0
```
Step 8 Enter the **show interface cable** command and verify that the card and line protocol is "up".

Example:

```
Router# show interface cable 8/0/0
Cable8/0/0 is up, line protocol is up
  Hardware is BCM3210 ASIC, address is 000a.13e8.1ca8 (bia 000a.13e8.1a60)
  Internet address is 10.1.1.3/24
  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation, loopback not set, keepalive not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 4d07h, 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 1834000 bits/sec, 2385 packets/sec
  5 minute output rate 1982000 bits/sec, 2431 packets/sec
      24461542 packets input, 2348214388 bytes, 0 no buffer
      Received 1979 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      24854257 packets output, 2536222931 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
      0 output buffer failures, 0 output buffers swapped out
```

Step 9 Enter the **show controllers cable** command and verify the hardware status.

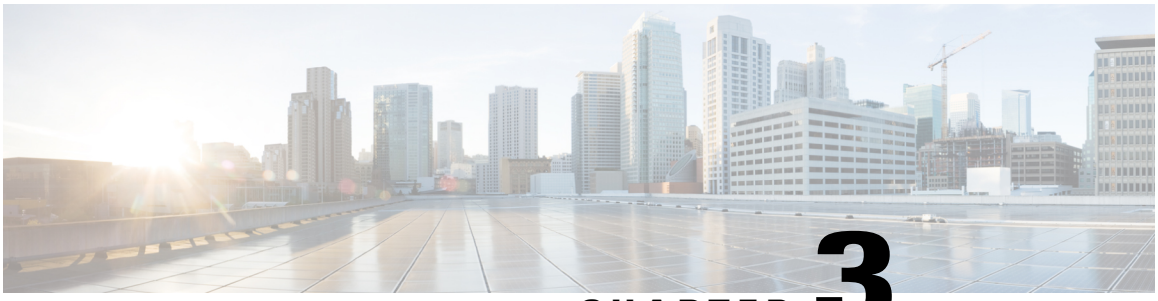
Example:

```
Router# show controllers cable 8/0/0
Cable8/0/0 JIB hardware status:
  JIB Downstream port   Enabled
  JIB Upstream   port 0 Enabled
  JIB Upstream   port 1 Enabled
  JIB Upstream   port 2 Enabled
  JIB Upstream   port 3 Enabled
Cable8/0/0 Upconverter is Enabled Output is Enabled
  Model: 74-3153-02 Serial Number: 0WAV090200A1 CLEI Code: FFFFFFFFFF
  HW Rev:    PC2D0109 SW Rev: 203, NVRAM Rev: 021 ECI numb
```

Step 10 Verify the configuration with the **show running-configuration** command.

Example:

```
Router# show running-configuration
```



CHAPTER 3

Unique Device Identifier Retrieval for the Cisco CMTS

First Published: February 14, 2008

Last Modified: February 09, 2009

The Unique Device Identifier (UDI) Retrieval feature provides the ability to retrieve and display the UDI information from any Cisco product that has electronically stored such identity information.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Unique Device Identifier Overview

Each identifiable product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have sub-entities like slots. An Ethernet switch might be a member of a super-entity like a stack. Most Cisco entities that can be ordered leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

Benefits of the Unique Device Identifier Retrieval Feature

- Identifies individual Cisco products in your networks.
- Reduces operating expenses for asset management through simple, cross-platform, consistent identification of Cisco products.
- Identifies PIDs for replaceable products.
- Facilitates discovery of products subject to recall or revision.
- Automates Cisco product inventory (capital and asset management).
- Provides a mechanism to determine the entitlement level of a Cisco product for repair and replacement service.

Product Item Descriptor for Cable Products

For information on the Product Item Descriptor (PID), see the product hardware installation guide available on Cisco.com.

Retrieving the Unique Device Identifier

To use UDI retrieval, the Cisco product in use must be UDI-enabled. A UDI-enabled Cisco product supports five required Entity MIB objects. The five Entity MIB v2 (RFC-2737) objects are:

- entPhysicalName

- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

Although the **show inventory** command may be available, using that command on devices that are not UDI-enabled will likely produce no output.

Enter the **show inventory** command to retrieve and display information about all of the Cisco products installed in the networking device that are assigned a PID, VID, and SN. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

```
Router# show inventory

NAME: "", DESCR: "uBR10000 chassis, Hw Serial#: SPE08450FQA, Hw Revision: 1.1"
PID: uBR10000 , VID: 1.1, SN: SPE08450FQA
NAME: "slot 0/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "Routing Processor"
PID: Routing Processor , VID: 1.0, SN: CAT09030GVK
NAME: "PRE_A:FastEthernet0/0/0", DESCR: "Network Management Ethernet"
PID: Network Management Ethernet, VID: , SN:
NAME: "", DESCR: "Temperature Sensor"
PID: Temperature Sensor, VID: , SN:
NAME: "", DESCR: "Forwarding Processor"
PID: Forwarding Processor, VID: 1.0, SN: CAT09030GBL
NAME: "slot 0/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 1/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 1/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 2/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "1gigethernet-1"
PID: 1gigethernet-1 , VID: 1.0, SN: CAB0542KX74
NAME: "GigabitEthernet2/0/0", DESCR: "Gigabit Ethernet MAC Controller"
PID: Gigabit Ethernet MAC Controller, VID: Unknown Rev, SN:
NAME: "slot 2/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 3/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "1oc12pos-1"
PID: 1oc12pos-1 , VID: 2.0, SN: CAB0437ECQU
NAME: "POS3/0/0", DESCR: "Skystone 4302 Sonet Framer"
PID: Skystone 4302 Sonet Framer, VID: 0xFFFF, SN:
NAME: "slot 3/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 4/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 4/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 5/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 5/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "MC520S_D_connector"
PID: MC520S_D_connector, VID: 1.1, SN: CAT08510MM0
NAME: "Cable5/1-MAC0", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC1", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC2", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC3", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
```

```
NAME: "Cable5/1-MAC4", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-US0", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US1", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US2", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US3", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US4", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US5", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US6", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US7", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US8", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US9", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US10", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US11", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US12", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US13", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US14", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US15", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US16", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US17", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US18", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US19", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-DS0", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS1", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS2", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS3", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS4", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "slot 6/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 6/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 7/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 7/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 8/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 8/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "Container for Power Supply"
PID: Container for Power Supply, VID: , SN:
NAME: "", DESCR: "Power Supply"
PID: Power Supply , VID: , SN:
NAME: "", DESCR: "Power Supply"
PID: Power Supply , VID: , SN:
NAME: "", DESCR: "Container for Fan Tray"
PID: Container for Fan Tray, VID: , SN:
NAME: "", DESCR: "Fan Tray"
```

```
PID: Fan Tray , VID: , SN:
NAME: "", DESCR: "Fan"
PID: Fan , VID: , SN:
NAME: "", DESCR: "Fan"
PID: Fan , VID: , SN:
NAME: "", DESCR: "Backplane"
PID: Backplane , VID: 1.1, SN: SPE08450FQA
```

For diagnostic purposes, the **show inventory** command can be used with the **raw** keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

Note The **raw** keyword option is primarily intended for troubleshooting problems with the **show inventory** command itself.

```
Router# show inventory raw

NMS-RACK9-UBR10K-1#sh inventory raw
NAME: "", DESCR: "uBR10000 chassis, Hw Serial#: SPE08450FQA, Hw Revision: 1.1"
PID: uBR10000 , VID: 1.1, SN: SPE08450FQA
NAME: "slot 0/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "Routing Processor"
PID: Routing Processor , VID: 1.0, SN: CAT09030GVK
NAME: "PRE_A:FastEthernet0/0/0", DESCR: "Network Management Ethernet"
PID: Network Management Ethernet, VID: , SN:
NAME: "", DESCR: "Temperature Sensor"
PID: Temperature Sensor, VID: , SN:
NAME: "", DESCR: "Forwarding Processor"
PID: Forwarding Processor, VID: 1.0, SN: CAT09030GBL
NAME: "slot 0/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 1/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 1/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 2/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "1gigethernet-1"
PID: 1gigethernet-1 , VID: 1.0, SN: CAB0542KX74
NAME: "GigabitEthernet2/0/0", DESCR: "Gigabit Ethernet MAC Controller"
PID: Gigabit Ethernet MAC Controller, VID: Unknown Rev, SN:
NAME: "slot 2/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 3/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "1oc12pos-1"
PID: 1oc12pos-1 , VID: 2.0, SN: CAB0437ECQU
NAME: "POS3/0/0", DESCR: "Skystone 4302 Sonet Framer"
PID: Skystone 4302 Sonet Framer, VID: 0xFFFF, SN:
NAME: "slot 3/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 4/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 4/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 5/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 5/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "MC520S_D_connector"
PID: MC520S_D_connector, VID: 1.1, SN: CAT08510MM0
NAME: "Cable5/1-MAC0", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC1", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC2", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
```

```
NAME: "Cable5/1-MAC3", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-MAC4", DESCR: "UBR10000 CLC"
PID: UBR10000 CLC , VID: 0x0 , SN:
NAME: "Cable5/1-US0", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US1", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US2", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US3", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US4", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US5", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US6", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US7", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US8", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US9", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US10", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US11", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US12", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US13", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US14", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US15", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US16", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US17", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US18", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-US19", DESCR: "LBT4522 PHY"
PID: LBT4522 PHY , VID: 4522, SN:
NAME: "Cable5/1-DS0", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS1", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS2", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS3", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "Cable5/1-DS4", DESCR: "BCM3033 PHY"
PID: BCM3033 PHY , VID: 3033, SN:
NAME: "slot 6/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 6/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 7/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 7/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 8/0/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "slot 8/1/0", DESCR: "Chassis Slot"
PID: Chassis Slot , VID: , SN:
NAME: "", DESCR: "Container for Power Supply"
PID: Container for Power Supply, VID: , SN:
NAME: "", DESCR: "Power Supply"
PID: Power Supply , VID: , SN:
NAME: "", DESCR: "Power Supply"
PID: Power Supply , VID: , SN:
NAME: "", DESCR: "Container for Fan Tray"
```

```
PID: Container for Fan Tray, VID: , SN:
NAME: "", DESCR: "Fan Tray"
PID: Fan Tray , VID: , SN:
NAME: "", DESCR: "Fan"
PID: Fan , VID: , SN:
NAME: "", DESCR: "Fan"
PID: Fan , VID: , SN:
NAME: "", DESCR: "Backplane"
PID: Backplane , VID: 1.1, SN: SPE08450FQA

NAME: "fan 1", DESCR: "Fan"
PID: , VID: , SN:
NAME: "fan 2", DESCR: "Fan"
PID: , VID: , SN:
NAME: "Backplane", DESCR: "Backplane"
PID: , VID: , SN: SPE08450FQA
```

Troubleshooting Tips

If any of the Cisco products do not have an assigned PID, the output may display incorrect PIDs and the VID and SN elements may be missing, as in the following example.

```
NAME: "POS3/0/0", DESCR: "Skystone 4302 Sonet Framer"

PID: FastEthernet, VID: , SN:

NAME: "Serial1/0", DESCR: "M4T"

PID: M4T                , VID:    , SN:
```

In the sample output, the PID is exactly the same as the product description. The UDI is designed for use with new Cisco products that have a PID assigned. UDI information on older Cisco products is not always reliable.

Additional References

Related Documents

Related Topic	Document Title
Information about managing configuration files	Cisco IOS Configuration Fundamentals Configuration Guide
Commands for showing interface statistics	Cisco IOS Interface Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2737	*Entity MIB (Version 2)*

MIBs

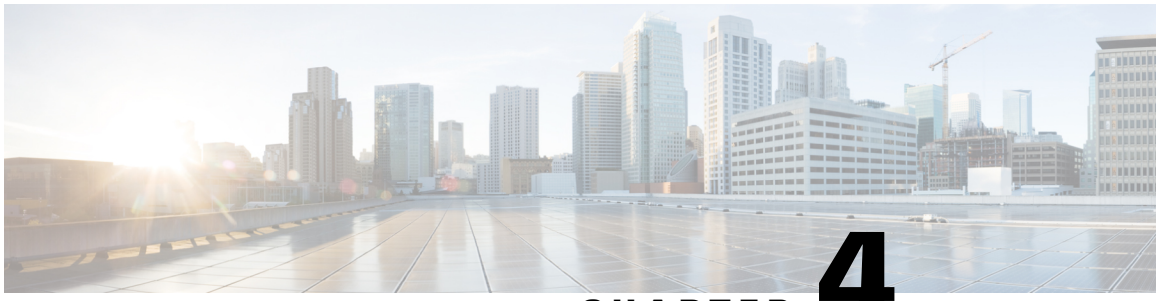
MIB	MIBs Link
CISCO-ENTITY-ASSET-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

PART II

CMTS Router Service Features



CHAPTER 4

Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The Advanced-Mode DOCSIS Set-Top Gateway (A-DSG) Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™, to include the following enhancements:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*
- A-DSG 1.2 introduces support for the DOCS-DSG-IF MIB.

Cisco A-DSG 1.2 is certified by CableLabs™, and is a powerful tool in support of latest industry innovations. A-DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the broadband cable environment. The set-top box (STB) dynamically learns the overall environment from the Cisco CMTS router, to include MAC address, traffic management rules, and classifiers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Advanced-Mode DSG Issue 1.2

Table below shows the hardware compatibility prerequisites for the A-DSG for the Cisco CMTS Routers feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 1: A-DSG for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V[1]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V[2]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V[3]

1 Cisco uBR3GX60V cable interface line card is compatible only with PRE4.
2 You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.
3 You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Advanced-Mode DSG Issue 1.2

This section contains restrictions that are specific to A-DSG 1.2 on a Cisco CMTS router.

DSG Configuration File Transfer Operations

DSG 1.2 does not support the copying of a DSG configuration file from a TFTP server, file system, or bootflash to the running configuration.

Previously, with DSG 1.1, when copying the DSG configuration file from a file system or TFTP server to the running configuration, DSG rule error checking may disable a previously configured and valid DSG tunnel configuration. This issue has not been observed in DSG 1.1 when loading the DSG configuration file from the startup configuration, as during a reload.

Multicast Configuration Restrictions

As with earlier versions of DSG Issues 0.9 and 1.0, IP multicasting must be configured for correct operation of A-DSG 1.2. Specifically, IP multicast routing must be set in global configuration. Also, IP PIM must be configured on all bundle interfaces of cable interfaces that are to carry multicast traffic.

See the Configuring the Default Multicast Quality of Service, on page 57 and the Configuring IP Multicast Operations, on page 63 for additional Multicast information and global configurations supporting DSG.

NAT for DSG Unicast-only Mapping

A-DSG 1.2 supports multicast IP addressing. However, it also supports unicast IP destination addresses. On the Cisco uBR7246VXR router, DSG 1.2 support is provided with the configuration of Network Address Translation (NAT) on the router, to include these settings:

- WAN interface(s) are configured with the **ip nat outside** command.
- Cable interface(s) are configured with the **ip nat inside** command.
- For each mapping, additional configuration includes the source static multicast IP address and the unicast IP address.

The unicast IP address is the unicast destination IP address of the DSG packets arriving at the Cisco CMTS router. The multicast IP address is the new destination IP address that is configured to map to one or a set of DSG tunnels.

PIM and SSM for Multicast

When using Source Specific Multicast (SSM) operation in conjunction with A-DSG 1.2, the following system-wide configuration command must be specified:

- **ip pim ssm**

Refer to the Configuring IP Multicast Operations, on page 63.

Subinterfaces

A-DSG 1.2 supports subinterfaces on the Cisco CMTS router starting from Cisco IOS Release 12.2(33)SCB4.

Note Effective with Cisco IOS Release 12.2(33)SCH3, ensure that the DSG downstream configuration is disabled, before you remove a DSG tunnel group from a subinterface.

Information About Advanced-Mode DSG Issue 1.2

A-DSG 1.2 offers substantial upgrades over A-DSG 1.1 and earlier basic DSG on the Cisco CMTS router. A-DSG 1.2 offers these new or enhanced capabilities:

- A-DSG client and agent modes
- Advanced-mode MIBs supporting DSG 1.2, including the DOCS-DSG-IF-MIB
- Advanced-mode tunnels with increased security
- Cable interface bundling through virtual interface bundling
- Downstream Channel Descriptor
- IP multicast support
- Quality of Service (QoS)

DSG 1.2 Clients and Agents

A-DSG 1.2 supports the DSG client and agent functions outlined by the CableLabs™ *DOCSIS Set-top Gateway (DSG) Interface Specification* , CM-SP-DSG-I05-050812.

FQDN Support

Starting with Cisco IOS Release 12.2(33)SCG, you can specify either a fully-qualified domain name (FQDN) or IP address for A-DSG classifier multicast group and source addresses using the **cable dsg cfr** command in global configuration mode. We recommend that you use an FQDN to avoid modification of multicast group and source addresses when network changes are implemented.

This feature allows you to use a hostname (FQDN) in place of the source IP address using the **cable dsg cfr** command. For example, you have two A-DSG tunnel servers, in two locations, sending multicast traffic to the same multicast address. In this scenario, you can specify a hostname for the source IP address and let the DNS server determine which source is sending the multicast traffic.

If you configure an A-DSG classifier with a hostname, the Cisco CMTS router immediately verifies if the hostname can be resolved against an IP address using the local host cache. If not, the router does not enable the classifier until the hostname is resolved. If the hostname cannot be resolved locally, the router performs a DNS query to verify the DSG classifiers.

The FQDN format does not support static Internet Group Management Protocol (IGMP) join requests initiated on the Cisco CMTS router. The IGMP static group IP address created automatically under a bundle interface at the time of A-DSG configuration is not displayed in the **show running-config interface command output i**n Cisco IOS Release 12.2(33)SCG and later. To display the A-DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode **i**n Cisco IOS Release 12.2(33)SCG and later.

DSG Name Process and DNS Query

Every DNS record contains a time to live (TTL) value set by the server administrator, and this may vary from seconds to weeks. The DSG name process supersedes the TTL value criterion to update A-DSG classifiers on the Cisco CMTS router.

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates. To enable the Cisco CMTS router to perform a DNS query for an A-DSG classifier verification, you must configure one or more DNS servers using the **ip name-server** command in global configuration mode. You can also specify the DNS query interval using the **cable dsg name-update-interval** command in global configuration mode.

During a Cisco IOS software reload or a route processor switchover, the router may fail to query the DNS server if the interfaces are down, and the router may not wait for the interval specified using the **cable dsg name-update-interval** command to perform a DNS query. In this case, for an unresolved hostname, the router automatically performs a DNS query based on a system-defined (15 seconds) interval to facilitate faster DSG classifier updates. You cannot change the system-defined interval.

A-DSG Forwarding on the Primary Channel

In Cisco IOS Release 12.2(33)SCF and earlier, DSG tunnels are configured globally and applied to all MAC domain interfaces. This automatically creates DSG tunnels for all primary capable interfaces associated with the MAC domain interfaces.

In Cisco IOS Releases earlier to 12.2(33)SCG, you cannot exclude A-DSG forwarding per primary capable interface. However, you can disable A-DSG forwarding for the entire MAC domain by using the no form of the cable dsg tg command.

Starting with Cisco IOS Release 12.2(33)SCG, you can disable A-DSG forwarding per primary capable interface using the **cable downstream dsg disable** command in interface configuration mode. Primary capable interfaces include modular, integrated cable interfaces, and Cisco uBR10-MC5X20 and Cisco uBR-MC28U cable interfaces.

For example, assume the cable interface 7/1/1 has A-DSG enabled and has four modular channels attached to it. However, you want A-DSG forwarding enabled only on two of these four modular channels. You can exclude the channels of your choice using the cable downstream dsg disable command. For details on how to disable modular channels, see the Disabling A-DSG Forwarding on the Primary Channel, on page 70.

Note If A-DSG downstream forwarding is disabled on a primary capable interface, the router does not create multicast service flows on the primary capable interface and stops sending Downstream Channel Descriptor (DCD) messages.

DOCSIS 3.0 DSG MDF Support

Support for DOCSIS 3.0 DSG Multicast DSID Forwarding (MDF) is introduced in Cisco IOS Release 12.2(33)SCG using DSG DA-to-DSID Association Entry type, length, value (TLV 13) in the MAC domain descriptor (MDD) message to communicate the association between a downstream service identifier (DSID) and a group MAC address used for DSG tunnel traffic. This is automatically supported on the Cisco CMTS router.

DOCSIS 2.0 hybrid CMs and DOCSIS 3.0 CMs use Dynamic Bonding Change (DBC) to get DSID information from the Cisco CMTS router, whereas DOCSIS 2.0 DSG hybrid embedded CMs and DOCSIS 3.0 DSG embedded CMs get DSID information from the Cisco CMTS router through MDD messages.

To disable MDF capability on all DSG embedded cable modems, including DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid modems, use the cable multicast mdf-disable command with the dsg keyword in global configuration mode.

Source Specific Multicast Mapping

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments.

The following two Cisco IOS components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Starting with Cisco IOS Release 12.2(33)SCG, SSM mapping can be configured on Cisco CMTS routers.

For details on how to configure SSM mapping on a Cisco CMTS router, see the Source Specific Multicast (SSM) Mapping feature guide.

How to Configure Advanced-Mode DSG Issue 1.2

Advanced-mode DSG Issue 1.2 entails support for DSG tunnel configuration, to include global, WAN-side, and interface-level settings in support of Multicast.

Configuring the Default Multicast Quality of Service

According to DOCSIS 3.0, you must configure the default multicast quality of service (MQoS) when using the MQoS. This also applies to the DSG, which uses the MQoS by associating a service class name with the tunnel.

If the default MQoS is not configured, the DSG tunnel service class configuration is rejected. Similarly, if no DSG tunnel uses the MQoS, you are prompted to remove the default MQoS.

The CMTS selects the primary downstream channel to forward the multicast traffic when the default MQoS is configured and there is no matching MQoS group configuration. Otherwise, the wideband interface is used to forward the multicast traffic.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn name1 aggregate`	Configures a service class name for the QoS profile.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Note If you configure or remove the default MQoS while the CMTS is sending multicast traffic, duplicate traffic is generated for approximately 3 minutes (or 3 times the query interval).

Configuring Global Tunnel Group Settings for Advanced-Mode DSG 1.2

This procedure configures global and interface-level commands on the Cisco CMTS router to enable DSG tunnel groups. A DSG tunnel group is used to bundle some DSG channels together and associate them to a MAC domain interface.

Global A-DSG 1.2 Tunnel Settings

This procedure sets and enables global configurations to support both A-DSG 1.2 clients and agents. Additional procedures provide additional settings for these clients and agents.

Before You Begin

Starting with the Cisco IOS Release 12.2(33)SCC1, when DOCSIS Set-top Gateway (DSG) is configured to have quality of service (QoS) for tunnel, ensure that the default multicast QoS (MQoS) is also configured. For more information, see Configuring the Default Multicast Quality of Service, on page 57.

Note The DSG tunnel service class configuration is rejected, if default MQoS is not configured.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**cable dsg tg***group-id* [**channel***channel-id* |**priority***DSG-rule-priority*] [**enable**|**disable**] **Example:** `Router(config)# cable dsg tg 1 channel 1 priority 1 enable`	Command allows the association of a group of tunnels to one or more downstream interfaces on the Cisco CMTS.
Step 4	**cabledsg tg***group-id* [**channel** *channel-id* [**ucid** *ID1*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 ucid 1`	Sets the upstream channel or channels to which the DSG 1.2 tunnel applies.

	Command or Action	Purpose
Step 5	**cable dsg tg** *group-id* [**channel** *channel-id* [**vendor-param** *vendor-group-id*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 vendor-param 1`	Sets the vendor-specific parameters for upstream DSG 1.2 channels.
Step 6	**cable dsg vendor-param** *group-id* **vendor** *vendor-index* **oui** *oui* **value** *value-in-TLV* **Example:** `Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB`	Configures vendor-specific parameters for A-DSG 1.2. To remove this configuration from the Cisco CMTS, use the no form of this command.
Step 7	**cable dsg chan-list** *list-index* **index** *entry-index* **freq** *freq* **Example:** `Router(config)# cable dsg chan-list 1 index 1 freq 47000000`	Configures the A-DSG 1.2 downstream channel list. The channel list is a list of DSG channels (downstream frequencies) that set-top boxes can search to find the DSG tunnel appropriate for their operation. To remove the A-DSG 1.2 channel list from the Cisco CMTS, us the no form of this command.
Step 8	**cable dsg timer inde** [**Tdsg1** *Tdsg1*] | [**Tdsg2** *Tdsg2*] | [**Tdsg3** *Tdsg3*] | [**Tdsg4** *Tdsg4*] **Example:** `Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4`	Configures the A-DSG 1.2 timer entry to be associated to the downstream channel, and encoded into the Downstream Channel Descriptor (DCD) message. To remove the cable DSG timer from the Cisco CMTS, use the no form of this command.
Step 9	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 71.

Adding DSG Tunnel Group to a Subinterface

This procedure adds a DSG tunnel group to a subinterface using the cable dsg tg group-id command. After adding the DSG tunnel-group to a subinterface, appropriate IP Internet Group Management Protocol (IGMP) static joins are created and forwarding of DSG traffic begins, if the downstream DSG is configured.

Note This feature is not supported on Cisco IOS Release 12.2(33)SCC.

Before You Begin

Cisco IOS Release 12.2(33)SCB4 or Cisco IOS Release 12.2(33)SCC1 or future release versions must be installed previously on the Cisco CMTS.

The downstream DSG should exist to create IGMP static joins.

Restriction You can associate a DSG tunnel group to only one subinterface within the same bundle interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**interface bundle***bundle-subif-number* **Example:** `Router(config)# interface bundle 11.2` `Router(config-subif)#`	Specifies the interface bundle and enters the subinterface configuration mode.
Step 4	**cable dsg tg***group-id* **Example:** `Router(config-subif)# cable dsg tg 1`	Adds a DSG tunnel group to a subinterface.
Step 5	end **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.

Configuring the DSG Client Settings for Advanced-Mode DSG 1.2

After the global configurations and DSG client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue DSG 1.2 client configurations.

Restriction The **in-dcd ignore** option is not supported by DSG-IF-MIBS specification.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable dsg client-list** *client-list-id* **id-index** *id* {**application-id** *app-id* | **ca-system-id** *sys-id* | **mac-addr** *mac-addr* | **broadcast** [*broadcast-id*]} **Example:** `Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd`	Sets the DSG client parameters. This command is changed from earlier Cisco IOS Releases, and for DSG 1.2, this command specifies the optional broadcast ID to client ID broadcast type and vendor specific parameter index.
Step 4	**cable dsg client-list** *client-list-id* **id-index** *id* [**vendor-param** *vendor-group-id*] **Example:** `Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1`	Sets vendor-specific parameters for the DSG client.
Step 5	**cable dsg tunnel** *tunnel id* **mac_addr** *mac addr* **tg** *tunnel-group* **clients** *client-list-id* [**enable** | **disable**] **Example:** `Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable`	This command is changed to associate a tunnel group and client-list ID to a DSG tunnel. Also, an optional QoS service class name can be associated to the tunnel. **Note** To associate a cable service class with an A-DSG tunnel on a Cisco CMTS router, use the cable dsg tunnel srv-class command in global configuration mode.
Step 6	**cable dsg cfr** *cfr index* [**dest-ip** {*ipaddr* |*hostname}]* [**tunnel** *tunnel-index*][**dest-port** *start end*]| [**priority** *priority*][**src-ip** {*ipaddr* |*hostname}* [**src-prefix-len** *length*]] [**enable** | **disable**] [**in-dcd** {**yes** | **no** | **ignore**}]	Specifies the DSG classifier index, with optional support for the DCD parameter, indicating whether or not to include the classifier in the DCD message.

	Command or Action	Purpose
	Example: `Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip ciscovideo.com src-prefix-len 24 enable`	**Note** The **ignore** option was added to the **in-dcd keyword from** Cisco IOS Release 12.2(33)SCD5 onwards. When you use the **ignore** option, the DSG classifier is not included in the DCD message.
Step 7	**end** **Example:** `Router(config)# end` `Router#`	Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 71.

Configuring Downstream DSG 1.2 Settings for Advanced-Mode DSG 1.2

When the global and client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue with DSG 1.2 downstream configurations.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot* /*port* |*slot* /*subslot*/*port* } **Example:** `Router(config)# interface cable 8/1/1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**cable downstream dsg tg** *group-id* **[channel** *channel-id]* **Example:** `Router(config-if)# cable downstream dsg tg 1 channel 1`	Associates the DSG tunnel group to the downstream interface. To remove this setting, use the **no** form of this command.
Step 5	**cable downstream dsg chan-list** *list-index* **Example:** `Router(config-if)# cable downstream dsg chan-list 2`	Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the **no** form of this command.
Step 6	**cable downstream dsg timer** *timer-index* **Example:** `Router(config-if)# cable downstream dsg timer 3`	Associates the DSG timer entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command.
Step 7	**cable downstream dsg vendor-param** *vsif-grp-id* **Example:** `Router(config-if)# cable downstream dsg vendor-param 2`	Associates A-DSG vendor parameters to a downstream to be included in the DCD message. To remove this configuration from the Cisco CMTS, use the no form of this command.
Step 8	**cable downstream dsg** [**dcd-enable** | **dcd-disable**] **Example:** `Router(config-if)# cable downstream dsg dcd-enable`	Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the **disable** form of this command.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring IP Multicast Operations

This section describes how to configure the operation of IP multicast transmissions on the cable and WAN interfaces on the Cisco CMTS. You should perform this configuration on each cable interface being used for DSG traffic and for each WAN interface that is connected to a network controller or Conditional Access (CA) server that is forwarding IP multicast traffic.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables multicast routing on the router.
Step 3	**ip pim ssm** {**default** | **range**{*access-list* | *word* }} **Example:** `Router(config)# ip pim ssm range 4`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command. **Note** When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.
Step 4	ip cef distributed **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding (CEF) on the route processor card. To disable CEF, use the no form of this command. For additional information about the **ip cef** command, refer to the following document on Cisco.com: • *Cisco IOS Switching Services Command Reference* , Release 12.3 http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for each interface bundle being used for DSG traffic.
Step 6	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} **Example:** `Router(config-if)# ip pim dense-mode`	Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature: **Note** You must configure this command on each interface that forwards multicast traffic.
Step 7	Repeat Step 5, on page 64 and Step 6, on page 64 for each cable interface that is being used for DSG traffic. Also repeat these steps on each W AN interface that is forwarding IP multicast traffic from the DSG network controllers and Conditional Access (CA) servers.	

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DNS Query and DSG Name Process

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates.

Before You Begin

Ensure that the IP DNS-based hostname-to-address translation is configured on the Cisco CMTS router using the **ip domain-lookup** command in global configuration mode. This is configured by default, and the status is not displayed in the running configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name cisco.com`	Sets the IP domain name that the Cisco IOS software uses to complete unqualified host names
Step 3	r **ip name-serve***server-address*[**multiple-server-addresses**] **Example:** `Router(config)# ip name-server 131.108.1.111`	Sets the server IP address.
Step 4	**cable dsg name-update-interval***minutes* **Example:** `Router(config)# cable dsg name-update-interval 10`	Sets the interval to check the DNS server for any FQDN classifier changes.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring NAT to Support Unicast Messaging

This section describes how to configure a Cisco CMTS router for Network Address Translation (NAT) to enable the use of IP unicast addresses for DSG messaging. This allows the Cisco CMTS router to translate incoming IP unicast addresses into the appropriate IP multicast address for the DSG traffic.

For the Cisco uBR10012 router, A-DSG 1.2 can use an external router that is close to the Cisco CMTS to support unicast messaging. In this case, the nearby router must support NAT, and then send the address-translated multicast IP packets to the Cisco CMTS.

Tip This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the Configuration Examples for Advanced-Mode DSG, on page 81.

Note The Cisco CMTS router supports NAT only when it is running an "IP Plus" (-i-) Cisco IOS software image. Refer to the release notes for your Cisco IOS release for complete image availability and requirements.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *wan-interface* **Example:** `Router(config)# interface FastEthernet0/0`	Enters interface configuration mode for the specified WAN interface.
Step 3	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Configures the WAN interface as the "outside" (public) NAT interface.
Step 4	**interface bundle** *bundle-number* **Example:** `Router(config-if)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle. **Note** This interface bundle should have previously been configured for DSG operations.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary`	Configures the cable interface with an IP address and subnet that should match the unicast address being used for DSG traffic. This IP address and its subnet must not be used by any other cable interfaces, cable modems, or any other types of traffic in the cable network.
Step 6	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Configures the cable interface as the “inside” (private) NAT interface.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**ip nat inside source static** *ip-multicast-address cable-ip-address* **Example:** `Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2`	Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.
Step 9	Repeat Step 2, on page 66 and Step 8, on page 67 for each cable interface to be configured for DSG unicast traffic.	
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Interfaces for Multicast Operations

In addition to basic WAN interface configuration on the Cisco CMTS, described in other documents, the following WAN interface commands should be configured on the Cisco CMTS to support IP multicast operations with A-DSG 1.2, as required.

- **ip pim**
- **ip pim ssm**
- **ip cef**

These commands are described in the Configuring IP Multicast Operations, on page 63, and in the following documents on Cisco.com.

For additional information about the **ip pim** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4* : Multicast, Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/iprmc_r.html

For additional information about the **ip pim ssm** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast* , Release 12.3 T

http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/ip3_i2gt.html

For additional information about the **ip cef** command, refer to the following document on Cisco.com:

- *Cisco IOS Switching Services Command Reference* , Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html

Configuring a Standard IP Access List for Packet Filtering

This section describes how to configure a standard IP access list so that only authorized traffic is allowed on the cable interface.

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 84.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .

	Command or Action	Purpose
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle.
Step 6	**ip access-group** *access-list* **Example:** `Router(config-if)# ip access-group 90`	(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface. **Note** Standard Access lists only allow one address to be specified in the earlier step. If you apply an outbound access-list with only the multicast address of the tunnel denied, then the DSG traffic is not allowed to pass. **Note** On the Cisco uBR10012 router, inbound access lists on the cable interface do not apply to multicast traffic, so they do not apply here. As a result, the Cisco uBR10012 requires that you use extended access lists that are blocked in the outbound direction for packets originating from the cable modem or CPE device on the network, and destined to the multicast group. The multicast group contains the classifiers associated with A-DSG 1.1 rules enabled on the interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to Privileged EXEC mode.

Configuring a Standard IP Access List for Multicast Group Filtering

This section describes how to configure a standard IP access list so that non-DOCSIS devices, such as DSG set-top boxes, can access only the authorized multicast group addresses and DSG tunnels.

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 84.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0`	Enters interface configuration mode for the specified cable interface.
Step 6	**ip igmp access-group** *access-list* [*version*] **Example:** `Router(config-if)# ip igmp access-group 90`	(Optional, but recommended) Configures the interface to accept traffic only from the associated access list, so that only authorized devices are allowed to access the DSG tunnels.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Disabling A-DSG Forwarding on the Primary Channel

You can disable A-DSG forwarding per primary capable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface modular-cable** *slot /subslot/port :interface-number* **Example:** `Router(config)# interface modular-cable 1/0/0:0`	Specifies the modular cable interface and enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference .
Step 3	**cable downstream dsg disable** **Example:** `Router(config-if)# cable downstream dsg disable`	Disables A-DSG forwarding and DCD messages on the primary capable interface.
Step 4	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature

This section describes the following commands that you can use to monitor and display information about the Advanced-mode DOCSIS Set-Top Gateway feature:

Displaying Global Configurations for Advanced-Mode DSG 1.2

The following commands display globally-configured or interface-level DSG settings, status, statistics, and multiple types of DSG 1.2 tunnel information.

show cable dsg cfr

To verify all DSG classifier details, such as the classifier state, source, and destination IP addresses, use the show cable dsg cfr command as shown in the following example:

```
Router# show cable dsg cfr
cfr id state resolved applied conflict dest-ip          src-ip
------------------------------------ ----------------- -----------------
```

```
1000   en    yes      yes     no       232.10.10.0       dsg-server-a
                                                         (40.0.0.30)
1010   en    yes      yes     no       232.10.10.10      dsg-server-b
                                                         (40.0.0.40)
2000   en    yes      yes     no       232.10.11.0       dsg-server-c
                                                         (40.0.0.50)
2010   en    no       no      no       232.10.11.10      non-exist-hostnam
                                                         (----)
3000   en    yes      yes     no       239.10.11.11      0.0.0.0
```

To verify details of a particular DSG classifier, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr 1010
cfr id state resolved applied conflict dest-ip           src-ip
------------------------------------ ----------------- ---------------
1010   en    yes      yes     no       232.10.10.10      dsg-server-b
                                                         (40.0.0.40)
```

To verify the detailed output for all DSG classifiers, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr verbose
Cfr Id                    : 1000
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
Tunnel Id                 : 1000
Dest Hostname             : ----
Dest Hostname IP          : ----
Dest IP                   : 232.10.10.0
Src Hostname              : dsg-server-a
Src Hostname IP           : 40.0.0.30
Src IP                    : 40.0.0.30
Src Prefix Length         : 32
Dest Port Start           : 2000
Dest Port End             : 13821
Priority                  : 1
In DCD                    : yes
Forwarded                 : 0
Received                  : 0
Cfr Id                    : 1010
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
Tunnel Id                 : 1010
Dest Hostname             : ----
Dest Hostname IP          : ----
Dest IP                   : 232.10.10.10
Src Hostname              : dsg-server-b
Src Hostname IP           : 40.0.0.40
Src IP                    : 40.0.0.40
Src Prefix Length         : 32
Dest Port Start           : 2000
Dest Port End             : 13821
Priority                  : 1
In DCD                    : yes
Forwarded                 : 0
Received                  : 0
Cfr Id                    : 2000
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
```

```
Tunnel Id               : 2000
Dest Hostname           : ----
Dest Hostname IP        : ----
Dest IP                 : 232.10.11.0
Src Hostname            : dsg-server-c
Src Hostname IP         : 40.0.0.50
Src IP                  : 40.0.0.50
Src Prefix Length       : 32
Dest Port Start         : 13822
Dest Port End           : 13822
Priority                : 1
In DCD                  : yes
Forwarded               : 0
Received                : 0
Cfr Id                  : 2010
State                   : enable
Resolved                : no
Applied                 : no
Conflict                : no
Conflict Cfr Id         : --
Error Code              : 0(DSG_CFR_ERR_NONE)
Tunnel Id               : 2010
Dest Hostname           : ----
Dest Hostname IP        : ----
Dest IP                 : 232.10.11.10
Src Hostname            : non-exist-hostname
Src Hostname IP         : ----
Src IP                  : 0.0.0.0
Src Prefix Length       : 32
Dest Port Start         : 2000
Dest Port End           : 13821
Priority                : 1
In DCD                  : yes
Forwarded               : 0
Received                : 0
Cfr Id                  : 3000
State                   : enable
Resolved                : yes
Applied                 : yes
Conflict                : no
Conflict Cfr Id         : --
Error Code              : 0(DSG_CFR_ERR_NONE)
Tunnel Id               : 3000
Dest Hostname           : ----
Dest Hostname IP        : ----
Dest IP                 : 239.10.11.11
Src Hostname            : ----
Src Hostname IP         : ----
Src IP                  : 0.0.0.0
Src Prefix Length       : 32
Dest Port Start         : 2000
Dest Port End           : 13821
Priority                : 1
In DCD                  : yes
Forwarded               : 0
Received                : 0
```

To verify the detailed output for a single DSG classifier, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr 1010 verbose
Cfr Id                  : 1010
State                   : enable
Resolved                : yes
Applied                 : yes
Conflict                : no
Conflict Cfr Id         : --
Error Code              : 0(DSG_CFR_ERR_NONE)
Tunnel Id               : 1010
Dest Hostname           : ----
Dest Hostname IP        : ----
Dest IP                 : 232.10.10.10
```

```
Src Hostname            : dsg-server-b
Src Hostname IP         : 40.0.0.40
Src IP                  : 40.0.0.40
Src Prefix Length       : 32
Dest Port Start         : 2000
Dest Port End           : 13821
Priority                : 1
In DCD                  : yes
Forwarded               : 0
Received                : 0
```

show cable dsg host

To verify the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host** command as shown in the following example:

```
Router# show cable dsg host
Host              IP Address      Reference  Last Update Time
dsgserver1        232.1.1.10      2          21:41 08/01/2011
dsgserver2        234.3.2.1       1          21:41 08/01/2011
dsgserver3        ----            1          never
dsgserver4        ----            1          never
dsgserver5        ----            1          never
dsgserver6        235.5.5.5       1          21:41 08/01/2011
dsgserver7        235.0.0.2       1          21:41 08/01/2011
```

To verify the verbose output of the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host** command as shown in the following example:

```
Router# show cable dsg host verbose
Host                    IP Address      Reference  Last Update Time
dsgserver1       232.1.1.10      2          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 2 dest-ip 232.1.1.125 tunnel 1 priority 0 src-ip a.b.c.d d...
  cable dsg cfr 3 dest-ip 232.1.1.125 tunnel 1 priority 10 src-ip a.b.c.d ...
dsgserver2       234.3.2.1       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 4 dest-ip aaabbccc priority 0 src-ip cccdddeee disable
dsgserver3       ----     1          never
  Cfrs:
  cable dsg cfr 4 dest-ip aaabbccc priority 0 src-ip cccdddeee disable
dsgserver4       235.0.0.2       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 24 dest-ip g2 priority 0 disable
dsgserver5        235.0.0.3       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 30 dest-ip g3 tunnel 1 priority 0 disable
```

show cable dsg tunnel

To display tunnel MAC address, state, tunnel group id, classifiers associated to tunnel and its state, use the **show cable dsg tunnel** command in privileged EXEC mode. This command also displays the number of interfaces to which a tunnel is associated, the clients associated, and the QoS service class name for all the configured tunnels.

The following example illustrates this command:

```
Router# show cable dsg tunnel
     tunnel              TG      cfr     tunnel   rule   client service
id  state mac-addr       id    id  state I/F    id state listId class
1      en 0100.5e01.0001 1     1      en C5/0   1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
2      en 0100.5e01.0002 1     2      en C5/0   2     en 2
```

```
3       en 0100.5e01.0003 1     3       en C5/0   3     en 3
4       en 0002.0002.0001 2     4       en C5/0   4     en 1
                                          C5/1    1     en 1
5       en 0002.0002.0002 2     5       en C5/0   5     en 2      DSG-Rate2
                                          C5/1    2     en 2
6       en 0002.0002.0003 2     9       en C5/0   6     en 21
                                          C5/1    3     en 21
```

show cable dsg tunnel ID

To display information for a given DSG tunnel, use the **show cable dsg tunnel** command, specifying the tunnel for which to display information.

show cable dsg tunnel *tunnel-id* [**cfr** | **clients** | **interfaces** | **statistics** | **verbose**]

- **cfr—**Shows DSG tunnel classifiers.
- **clients—**Shows DSG tunnel clients.
- **interfaces—**Shows DSG tunnel interfaces.
- **statistics—**Shows DSG tunnel statistics.
- **verbose—**Shows DSG tunnel detail information.

The below example illustrates this command for DSG Tunnel 1:

```
Router# show cable dsg tunnel 1
     tunnel              TG      cfr     tunnel   rule   client service
id  state mac-addr       id    id  state I/F    id state listId class
1       en 0100.5e01.0001 1     1       en C5/0   1     en 1      DSG-Rate1
                                6       en
                                7       en
                                8       en
```

The below example shows detailed information of all the classifiers associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 cfr
tunnel cfr   cfr   cfr destination ip   source ip        srcPre d_port d_port
id     id    state pri address          address          length start  end
1      1     en    0   230.1.0.1        0.0.0.0          32     0      65535
       6     en    0   231.1.1.6        0.0.0.0          32     0      65535
       7     en    0   231.1.1.7        0.0.0.0          32     0      65535
       8     en    0   231.1.1.8        0.0.0.0          32     0      65535
```

The below example illustrates detailed information about all the clients associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 clients
tunnel client client client          client          vendor
id     listId id     id type         address         group
1      1      1      MAC Addr        0100.5e00.0001
              2      Application ID  0x0951
              3      Broadcast       Unspecified
              4      Broadcast       4
```

The below example illustrates all DSG interfaces and rules associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 interfaces
tunnel downstream   rule
id     interface    id
4      Cable5/0     4
       Cable5/1     1
```

show cable dsg tunnel ID statistics

The below example illustrates packet statistics information about the specified tunnel.

```
Router# show cable dsg tunnel 1 statistics
tunnel cfr   cfr   destination ip  source ip       total          total
id     id    state address         address         forwarded      received
1      1     en    230.1.0.1       0.0.0.0         0              0
       6     en    231.1.1.6       0.0.0.0         0              0
       7     en    231.1.1.7       0.0.0.0         0              0
       8     en    231.1.1.8       0.0.0.0         0              0
```

The below example illustrates all detailed information about the specified tunnel.

```
Router# show cable dsg tunnel 1 verbose
Tunnel ID                                       : 1
State                                           : enable
MAC Addr                                        : 0100.5e01.0001
TG Id                                           : 1
Cfr Id                                          : 1
State                                           : enable
Priority                                        : 0
Dest IP                                         : 230.1.0.1
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 6
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.6
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 7
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.7
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 8
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.8
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Client List Id                                  : 1
Client Id                                       : 1
Client Id Type                                  : MAC Addr        0100.5e00.0001
Client Id                                       : 2
Client Id Type                                  : Application ID  0x0951
Client Id                                       : 3
Client Id Type                                  : Broadcast       Unspecified
Client Id                                       : 4
Client Id Type                                  : Broadcast       4
Interface                                       : Cable5/0
Rule Id                                         : 1
```

show cable dsg tg

The below example illustrates configured parameters for all DSG tunnel groups.

```
Router# show cable dsg tg
TG    Chan  Chan         Rule Vendor UCID
id    id    state I/F    pri  Param  list
1     1     en    C5/0   16   1      1 2 3 4
1     2     en           0
2     1     en    C5/0   11   2
                  C5/1
2     2     en           0
```

Note Beginning with Cisco IOS Release 12.2(33)SCG, the "TG state" field in the **show cable dsg tg command output was replaced by "Chan state" to indicate that a channel belonging to a tunnel group is either enabled or diabled. It is possible that a tunnel group is enabled but a particular channel in that tunnel group is disabled.**

The below example displays the same information as above for the specified tunnel group.

```
Router# show cable dsg tg 1 channel 1
TG    Chan  Chan         Rule Vendor UCID
id    id    state I/F    pri  Param  list
1     1     en    C5/0   16   1      1 2 3 4
```

The below example illustrates detailed information for the specified tunnel group.

```
Router# show cable dsg tg 1 channel 1 verbose
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                        cfr                       clients
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

The following is a sample output for the **show cable dsg tg** command that displays the ignore option, introduced in Cisco IOS Release 12.2(33)SCD5, under the 'In DCD' column.

```
Router# show cable dsg tg 1 channel 1 verbose
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                        cfr                       clients
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
------ -------- ----------------------- ------------------------- --- -------
 C7/0/0 1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       ign    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

show running-config interface

To display a tunnel group attached to a subinterface, use the **show running-config interface** command in privileged EXEC mode, as shown in the example below:

```
Router# show running-config interface bundle 11.2
!
interface Bundle11.2
 ip address 4.4.2.1 255.255.255.0
```

```
 no ip unreachables
 ip pim sparse-mode
 ip igmp static-group 230.1.1.30
 no cable ip-multicast-echo
 cable dsg tg 61
end
```

Note The IGMP static group IP address created automatically at the time of DSG configuration is not displayed in the **show running-config interface command output i**n Cisco IOS Release 12.2(33)SCG and later.

show cable dsg static-group bundle

To verify all DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode as shown in the following example:

```
Router# show cable dsg static-group bundle 2
Bundle Interface     Group           Source
Bundle2              228.0.0.1       0.0.0.0
Bundle2              228.0.0.1       1.2.3.4
Bundle2              232.1.1.1       2.3.4.5
```

Displaying Interface-level Configurations for Advanced-Mode DSG 1.2

The following **show** commands display interface-level configurations for A-DSG 1.2.

show cable dsg tunnel interfaces

To display all interfaces and DSG rules for the associated tunnel, use the **show cable dsg tunnel interfaces** command in privileged EXEC mode.

show cable dsg tunnel (*tunnel-id*) **interfaces**

The following example illustrates this command:

```
Router# show cable dsg tunnel 1 interfaces
tunnel downstream   rule
id     interface    id
4      Cable5/0     4
       Cable5/1     1
```

show interfaces cable dsg downstream

To display DSG downstream interface configuration information, to include the number of DSG tunnels, classifiers, clients, and vendor-specific parameters, use the **show interfaces cable dsg downstream** command in privileged EXEC mode.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream**

Keywords for this command include the following:

- **dcd—**Displays the DSG downstream DCD message.
- **tg—**Displays the DSG downstream tunnel group.
- **tunnel—**Displays the DSG downstream tunnel.

The following example illustrates this command supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream
chan chFreq chan timer init    oper    twoWay oneWay num  num    num  num    num
list index  freq index timeout timeout timer  timer  rule tunnel cfr  client vsp
1    1      471  1     4       600     300    1800   6    6      3    4      2
     2      477
     3      483
     4      583
```

show interfaces cable dsg downstream dcd

To display DCD statistics for the given downstream, use the **show interfaces cable dsg downstream dcd** command in privileged EXEC mode. This command only displays DCD Type/Length/Value information if the **debug cable dsg** command is previously enabled.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream dcd**

The following example illustrates DCD statistics information supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream dcd
dcd   dcd   num of dcd           num of dcd           num of dcd  num of
state Tx    sent                fail                 change cnt  fragment
en    on    6502                0                    28          1
Router# debug cable dsg
CMTS DSG debugging is on
Router#
Router# show interfaces c5/0 dsg downstream dcd
dcd   dcd   num of dcd           num of dcd           num of dcd  num of
state Tx    sent                fail                 change cnt  fragment
en    on    6512                0                    28          1
Router#
02:08:42: DCD TLV last sent:
32360101 01020110 03040102 03040412 02060100 5E000001 04020951 01000102
00040506 01005E01 00010602 00012B08 08030000 01010101 170F0202 00010501
00090605 04E60100 01322801 01020201 10030401 02030404 0403020A BC050601
005E0100 02060200 022B0808 03000001 01010117 0F020200 02050100 09060504
E6010002 32280101 03020110 03040102 03040404 04020123 05060100 5E010003
06020003 2B080803 00000101 0101170F 02020003 05010009 060504E6 01000332
38010104 02010B04 12020601 005E0000 01040209 51010001 02000405 06000200
0200012B 09080300 00010102 01022B09 08030000 02010201 02322A01 01050201
0B040403 020ABC05 06000200 0200022B 09080300 00010102 01022B09 08030000
02010201 02324601 01060201 0B042002 06002100 21000102 06002100 21000202
06002100 21000302 06002100 21000405 06000200 0200032B 09080300 00010102
01022B09 08030000 02010201 02332801 041C12E3 C001041C 6E714001 041CC9FE
C0010422 BFDFC002 02000403 02025804 02012C05 020708
```

show interfaces cable dsg downstream tg

To display DSG tunnel group parameters, and rule information applying to the tunnel group, to include tunnels and tunnel states, classifiers, and client information, use the **show interfaces cable dsg downstream tg** command in privileged EXEC mode. You can display information for a specific tunnel, if specified.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream tg [channel** *channel-id***]**

The following example illustrates typical information displayed with this command in DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream tg
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                       client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
```

```
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
TG: 2     Chan: 1     state: en pri: 11 Vendor: 2     UCID:
          rule        tunnel                    cfr                      client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   4     en 4     en 0002.0002.0001 4      en 230.2.2.1       no     1
        5     en 5     en 0002.0002.0002 5      en 230.2.2.2       no     2
        6     en 6     en 0002.0002.0003 9      en 231.1.1.9       no     21
```

The following examples displays the same type of information as above for the given tunnel group.

```
Router# show interfaces c5/0 dsg downstream tg 1 channel 1
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                      client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

The following is a sample output for the **show interfaces cable dsg downstream tg** command that displays the ignore option, introduced in Cisco IOS Release 12.2(33)SCD5, under the 'In DCD' column.

```
Router# show interfaces cable 7/0/0 dsg downstream tg
TG: 1     Chan: 1     State: en  Pri: 0   Vendor:       UCID:
   rule        tunnel                    cfr              In  clients
 id state id  state mac-addr       id  state dest-ip         DCD listId
 -------- ---------------------- ---------------------- --- -------
 1     en 1      en 0100.5e01.0101 1      en 230.1.1.1       ign  1
```

show interfaces cable dsg downstream tunnel

To display DSG tunnel information associated with the downstream, use the **show interfaces cable dsg downstream tunnel** command in privileged EXEC mode.

show interfaces cable {*slot*/*port* | *slot*/*subslot*/*port*} **dsg downstream tunnel***tunnel-id*

The following is a sample output for the **show interfaces cable dsg downstream tunnel** command that displays the interface information for the DSG downstream tunnel in DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream tunnel
     tunnel              TG      cfr       rule   client service
id  state mac-addr       id    id  state id state listId class
1      en 0100.5e01.0001 1     1      en 1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
2      en 0100.5e01.0002 1     2      en 2     en 2
3      en 0100.5e01.0003 1     3      en 3     en 3
4      en 0002.0002.0001 2     4      en 4     en 1
5      en 0002.0002.0002 2     5      en 5     en 2      DSG-Rate2
6      en 0002.0002.0003 2     9      en 6     en 21
```

The following is a sample output for the **show interfaces cable dsg downstream tunnel** command that displays information for the specified interface and tunnel:

```
Router# show interfaces c5/0 dsg downstream tunnel 1
     tunnel              TG      cfr       rule   client service
id  state mac-addr       id    id  state id state listId class
1      en 0100.5e01.0001 1     1      en 1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
```

Debugging Advanced-Mode DSG

To enable debugging for A-DSG on a Cisco CMTS router, use the debug cable dsg command in privileged EXEC mode.

Configuration Examples for Advanced-Mode DSG

This configuration example illustrates a sample DSG network featuring these components:

- Two Cisco universal broadband routers
- IP Multicast for each DSG implementation
- Two DSG Clients for each Cisco CMTS
- Two DSG Servers (one for each Cisco CMTS)

Each Cisco CMTS is configured as follows, and the remainder of this topic describes example configurations that apply to this architecture.

CMTS Headend 1

- DSG Server #1—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.1
- Destination IP Address for the Cisco CMTS—228.9.9.1
- DSG Tunnel Address—0105.0005.0005
- Downstream #1 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

CMTS Headend 2

- DSG Server #2—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.2
- Destination IP Address for the Cisco CMTS—228.9.9.2
- DSG Tunnel Address—0106.0006.0006
- Downstream #2 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

Example of Two DSG Tunnels with MAC DA Substitution

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5

These settings apply to DSG Rule #2 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6

DSG Example with Regionalization Per Downstream

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two downstream rules that can be configured in this architecture, for example:

- Downstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG Tunnel Address—105.5.5
- Downstream Rule #2
  - DSG Rule ID #2
  - DSG Client ID—102.2.2
  - DSG Tunnel Address—106.6.6

DSG Example with Regionalization Per Upstream

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two upstream rules that can be configured in this architecture, for example:

- Upstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG UCID Range—0 to 2
  - DSG Tunnel Address—105.5.5
- Upstream Rule #2
  - DSG Rule ID #2
  - DSG Client ID—102.2.2
  - DSG UCID Range—3 to 5

- DSG Tunnel Address—106.6.6

Example of Two DSG Tunnels with Full Classifiers and MAC DA Substitution

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10
- IP SA—12.8.8.1
- IP DA—228.9.9.1
- UDP DP—8000

These settings apply to DSG Rule #2:

- DSG Rule ID 2
- Downstreams 1 and 2
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6
- DSG Classifier ID—20
- IP SA—12.8.8.2
- IP DA—228.9.9.2
- UDP DP—8000

Example of One DSG Tunnel Supporting IP Multicast from Multiple DSG Servers

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below is an example of one DSG Tunnel with multiple DSG servers supporting IP Multicast:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1 and 102.2.2
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10
    - IP SA—12.8.8.1
    - IP DA—228.9.9.1

- UDP DP—8000

- DSG Classifier ID—20
  - IP SA—12.8.8.2
  - IP DA—228.9.9.2
  - UDP DP—8000

Example: Enabling DNS Query

The following example shows how to enable a DNS query on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ip domain-lookup
Router(config)# ip domain-name cisco.com
Router(config)# ip name-server 131.108.1.111
Router(config)# cable dsg name-update-interval 10
Router(config)# end
```

Example: Disabling A-DSG Forwarding on the Primary Channel

The following example shows how to disable A-DSG forwarding on a primary capable modular interface on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable downstream dsg disable
Router(config-if)# end
```

Additional References

The following sections provide references related to A-DSG 1.2.

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
DOCSIS 3.0 Multicast Support on the CMTS Routers	DOCSIS 3.0 Multicast Support on the CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_d30_mcast_support.html

Standards

Standard	Title
CM-SP-DSG-I18-110623	DOCSIS Set-top Gateway (DSG) Interface Specification

MIBs

MIB	MIBs Link
DOCS-DSG-IF-MIB	*To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:* http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Advanced-Mode DSG 1.2 for the Cisco CMTS Routers

Table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

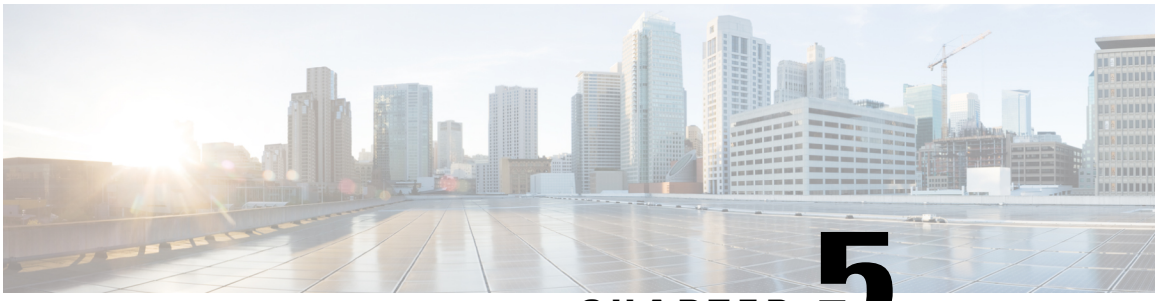
Note Table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for DOCSIS Set-Top Gateway and A-DSG for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	12.2(15)BC2	This feature was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	12.3(9a)BC	Support for the Cisco uBR10012 universal broadband router was added.
Advanced-mode DOCSIS Set-Top Gateway 1.1 for the Cisco CMTS Routers	Release 12.3(13)BC	This feature was introduced to support DOCSIS 1.1 on the Cisco uBR7200 Series and Cisco uBR10012 universal broadband routers.
Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers	12.3(17a)BC2	This feature was introduced on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR universal broadband router was added.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCB4	This feature was introduced on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
Default Multicast QoS	12.2(33)SCC1	This feature was modified to configure the service class name of the default multicast quality of service (MQoS) for the QoS profile. The following command was introduced or modified: • cable multicast group-qos default

Feature Name	Releases	Feature Information
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCC1	This feature was integrated into Cisco IOS Release 12.2(33)SCC1.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCD	Support was added for the Cisco uBR-MC88V line card.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCD5	This feature was modified to add the **ignore** option to the **in-dcd** keyword of the **cable dsg cfr** command to exclude DSG classifiers from the DCD message and enable the DSG rules regardless of the DSG tunnel MAC address. The following commands were introduced or modified: • **cable dsg cfr** • **show cable dsg tg** • **show interfaces cable dsg downstream tg**
FQDN Support	12.2(33)SCG	You can specify either an FQDN or IP address while configuring an A-DSG classifier on a Cisco CMTS router. The following commands were introduced or modified: • **cable dsg cfr** • cable dsg tg default-priority • cable dsg tg priority • debug cable dsg • show cable dsg cfr • show cable dsg host

Feature Name	Releases	Feature Information
DNS Query and DSG Name Process	12.2(33)SCG	One or more DNS servers must be configured to enable a Cisco CMTS router to perform a DNS query. The **cable dsg name-update-interval command** was introduced to support this feature. The following sections provide information about this feature:
DOCSIS 3.0 DSG MDF Support	12.2(33)SCG	DOCSIS 3.0 DSG MDF support is introduced using DSG DA-to-DSID Association Entry TLV in the MDD message. For details about this feature, see Information About Advanced-Mode DSG Issue 1.2, on page 54.
A-DSG Forwarding on the Primary Channel	12.2(33)SCG	This feature allows you to exclude a primary capable interface from A-DSG forwarding. The following sections provide information about this feature: The following commands were introduced or modified: • **cable downstream dsg disable** • **cable downstream dsg tg** • show cable dsg static-group bundle • show interface cable dsg downstream



CHAPTER 5

Call Home Feature for the Cisco CMTS Routers

First Published: November 29, 2010

Note Use this document in conjunction with the Configuring Call Home for Cisco 7200 Series Routers feature guide.

For Cisco IOS Release 12.2(33)SCE, the Call Home feature provides a mechanism to automatically create cases and update Cisco, customer, or a partner about events and changes on a Cisco device in a customer network. This feature provides e-mail and web-based notification of critical system events. Multiple message formats are available for optimum compatibility with pager services, e-mail, or XML-based automated parsing applications. Common uses of this feature include paging a network support engineer, sending an e-mail notification to a Network Operations Center, XML-based message delivery to a support website, and generating a direct case with the Cisco Systems Technical Assistance Center (TAC).

For more information, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Call Home Feature for the Cisco CMTS Routers

Table below shows the hardware compatibility matrix for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 3: Call Home Feature for the Cisco CMTS Routers - Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCE and later releases • PRE2 • PRE4	Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR10-MC5X20U/H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V [4]	Cisco Wideband SPA

4 The Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

Note For support of this feature on the Cisco uBR 7200 series universal broadband routers, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

Information About the Call Home Feature for the Cisco CMTS Routers

The Call Home feature provides a reactive support mode of operation triggered by various system events on a Cisco uBR10012 universal broadband router. This feature also supports a proactive support mode where configuration and inventory change messages are automatically reported to a destination target specified in the system profile.

You can specify a Call Home Server on the Cisco network as a destination target.

The Call Home functionality in a Cisco device is provided by one or more network devices or through an appliance, such as the Smart Call Home server. Each system event provides a set of call home triggers required for reactive mode situations, for example, hardware failures.

The Call Home function can leverage Cisco, customer, or a partner support. Flexible message delivery and format options allow for easy integration of specific support requirements into the Call Home and Call Home Server.

For more information on setting up and configuring this feature, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts supported in all Cisco universal broadband routers. Different Call Home alerts are classified into different groups depending on their type. For Cisco IOS Release 12.2(33)SCE, the alert groups are:

- Configuration
- Inventory
- Syslog

Sample Configuration Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MC2:SPE100202ZH:D060082A</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/configuration</aml-block:Type>
<aml-block:CreationDate>2010-10-13 10:27:54 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>uBR10000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GC3:SPE100202ZH:D060082A</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:27:39 GMT+00:00</ch:EventTime>
<ch:MessageDescription>Configuration Change</ch:MessageDescription>
<ch:Event>
<ch:Type>configuration</ch:Type>
<ch:SubType>delta</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
```

```
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GC3:SPE100202ZH:D060082A</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:27:39 GMT+00:00</ch:EventTime>
<ch:MessageDescription>Configuration Change</ch:MessageDescription>
<ch:Event>
<ch:Type>configuration</ch:Type>
<ch:SubType>delta</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>UBR10012</rme:Model>
<rme:HardwareVersion>257</rme:HardwareVersion>
<rme:SerialNumber>SPE100202ZH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-09026-03" />
<rme:AD name="SoftwareVersion" value="12.2(20100929:171810)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.317" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M),
 Experimental Version 12.2(20100929:171810) [username-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by username" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show diag</aml-block:Name>
<aml-block:Data encoding="plain">
```

```
<![CDATA[
Slot A:
 Active PRE card
RP EEPROM contents:
 Controller Type          : 1443
 Hardware Revision        : 1.0
 PCB Part Number          : 73-10867-03
 Board Revision           : B0
 Deviation Number         : 0-0
 Fab Version              : 05
 PCB Serial Number        : CAT1336F051
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 Top Assy. Part Number    : 800-28163-03
 CLEI Code                : IPUCAM3BAC
 Product Identifier (PID) : ESR-PRE4
 Version Identifier (VID) : V03
FP EEPROM contents:
 Controller Type          : 1442
 Hardware Revision        : 1.0
 PCB Part Number          : 73-10866-03
 Board Revision           : B0
 Deviation Number         : 0-0
 Fab Version              : 04
 PCB Serial Number        : CAT1403F1JT
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
Operational Image Version, Slot A
 Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [uname-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by uname
Reset reason 0x00000002 (software reset)
Slot B:
 Standby PRE card
RP EEPROM Contents:
Slot 1:
 2jacket-1 card, 0 ports
 Card is full slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 43 minutes, 51 seconds
 Card idle time 1 days, 11 hours, 59 minutes, 24 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal 1.5V Nominal 12V Nominal
EEPROM contents, slot 1/0:
 Controller Type          : 1045
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-22843-04
 Board Revision           : A0
 Product Identifier (PID) : UBR10-2XDS-SIP
 Version Identifier (VID) : V01
 Deviation Number         : 89768
 Fab Version              : 03
 PCB Serial Number        : CAT112358KV
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 CLEI Code                : IPUIA1HRAA
LCMON version, slot 1/0
 LCDOS (C10000 PowerQUICC-II Line Card MONitor Image Version 2 : Release
branch:c10k_lc_conn_isp 20040915:175538)
 Built by leccese at Thu Sep 16 12:28:56 2004.
 Reset reason 0x00000003/0x2 (PRE hard reset).
Operational Image version, slot 1/0
 LCDOS (C10000 2 Bay SPA Jacket (JACKET2) Image : DEVELOPMENT BUILD
Wideband Information:
Slot/Subslot 1/1:
 24rfchannel-spa-1 card, 1 port + 1 redundant port
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
```

```
 Card uptime: Not Supported
 Card idle time: Not Supported
 Voltage status: 3.3V (+3.291) NOMINAL  2.5V (+2.490) NOMINAL
                 1.2V (+1.196) NOMINAL  1.8V (+1.806) FIXED
EEPROM contents, slot 1/1:
 Controller Type          : 1198
 Hardware Revision        : 1.0
 Boot Timeout             : 500 msecs
 PCB Serial Number        : CAT1228E21D
 PCB Part Number          : 73-9597-03
 PCB Revision             : B0
 Fab Version              : 03
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 Deviation Number         : 0
 Product Identifier (PID) : SPA-24XDS-SFP
 Version Identifier (VID) : V01
 Top Assy. Part Number    : 68-2562-03
 Top Assy. Revision       : C0
 IDPROM Format Revision   : 36
 System Clock Frequency   : 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00
 CLEI Code                : IPUIA1JRAA
 Base MAC Address         : 00 1E BE BE 8B C7
 MAC Address block size   : 1
 Manufacturing Test Data  : 00 00 00 00 00 00 00 00
 Field Diagnostics Data   : 00 00 00 00 00 00 00 00
 Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
       Calibration values :
 Power Consumption        : 14000 mWatts (Maximum)
 Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                            46 32 00 00 00 00 04 B0
                            46 32 00 00 00 00 07 08
                            46 32 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 FE 02 FA 6D
 Processor Label          : 00 00 00 00 00 00 00
 Platform features        : 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
 Asset ID                 :
 Asset Alias              :
Slot/Subslot 2/1:
 2cable-dtcc card, 0 ports
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 52 minutes, 34 seconds
 Card idle time 1 days, 5 hours, 1 minutes, 14 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal 1.8V Nominal 1.2V Nominal
EEPROM contents, slot 2/1:
 Controller Type          : 1456
 Hardware Revision        : 2.0
 Top Assy. Part Number    : 800-29390-01
 Top Assy. Revision       : A0
 Product Identifier (PID) : UBR10-DTCC
 Version Identifier (VID) : V01
 CLEI Code                : IPUCAL1BAA
 Deviation Number         : 0
 Fab Version              : 02
 PCB Serial Number        : CAT1213E19M
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
<snip>...</snip>
Slot/Subslot 4/0:
 1gigethernet-hh-1 card, 1 port
 Card is half slot size
 Card is analyzed
```

```
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 44 minutes, 31 seconds
 Card idle time 1 days, 16 hours, 12 minutes, 52 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal
EEPROM contents, slot 4/0:
 Controller Type          : 912
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-20373-03
 Board Revision           : A0
 Deviation Number         : 0-0
 Fab Version              : 03
 PCB Serial Number        : CAT09190TTY
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 CLEI Code                : IP3IZ0VDAB
LCMON version, slot 8/0
 Cisco IOS Software, 10000 Software (UBR10KG4CLC-EBOOT-M), Version 12.2(32.7.22)SCE  Compiled
 Thu 17-Jun-10 02:39
 Reset due to: reload
Operational Image version, slot 8/0
 Cisco IOS Software, 10000 Software (UBR10KG4CLC-LCK8-M), Experimental Version
12.2(20101012:185925) [yiliu-cable-1012 120]
 Compiled Wed 13-Oct-10 14:54
 SW Version 1.0
 Code MD5 B0DCEC92BF050F9D0A22131AB8AB4E14
 FPGA MD5 00000000000000000000000000000000
 Expected Switchover Action: NO INFORMATION
Slot/Subslot 8/1:
 ubr10k-clc-3g60 card, 15 ports
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 0 days, 1 hours, 37 minutes, 46 seconds
 Card idle time N/A
 Voltage status: 3.3V Nominal 2.5V Nominal 1.8V Nominal 1.5V Nominal 1.2V Nominal 1.0V
Nominal 1.0V Nominal 1.1V Core Nominal 1.1V Cpu Plat Nominal
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show version</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [uname-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by username
ROM: System Bootstrap, Version 12.2(20071113:194412) [uname-rom-1_2 101], DEVELOPMENT
SOFTWARE
BOOTLDR: Cisco IOS Software, 10000 Software (C10K4-EBOOT-M), Version 12.2(33)SB7, RELEASE
SOFTWARE (fc3)
 router uptime is 2 days, 6 hours, 45 minutes
Uptime for this control processor is 2 days, 6 hours, 45 minutes
System returned to ROM by reload at 06:03:47 UTC Wed Oct 6 2010
System image file is "tftp://223.255.254.254/uname/ubr10k4-k9p6u2-mz.card"
Last reload type: Normal Reload
Last reload reason: Reload command
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco uBR10000 (PRE4-RP) processor with 2588671K/163839K bytes of memory.
Processor board ID SPE100202ZH
SB-1 CPU at 800Mhz, Implementation 0x410, Rev 5.0, 512KB L2 Cache
Backplane version 1.1, 8 slot
Last reset from software reset
PXF processor tmc0 is running.
PXF processor tmc1 is running.
```

```
PXF processor tmc2 is running.
PXF processor tmc3 is running.
1 Jacket card(s): 1 SPA card(s)
1 FastEthernet interface
1 Gigabit Ethernet interface
40 Cable Modem interfaces
7039K bytes of non-volatile configuration memory.
126000K bytes of ATA compact flash in bootflash (Sector size 512 bytes).
1000944K bytes of ATA compact flash in disk0 (Sector size 512 bytes).
Configuration register is 0x0
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show running-config all</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Building configuration...
Current configuration with default configurations exposed : 876387 bytes
!
...<-- Running config information here -->
...
...
Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Sample Inventory Alert Notification in Long-Text Format

```
TimeStamp : 2010-04-01 20:45 GMT+00:00
Message Name : inventory
Message Type : Call Home
Message Group : reactive
Severity Level : 1
Source ID : uBR7200 Family
Device ID : Cisco-uBR7246VXR@C@SAB044900Q0
Customer ID :
Contract ID :
Site ID :
Server ID : Cisco-uBR7246VXR@C@SAB044900Q0
Event Description : Module 35: UBR-MC28U is removed
System Name : router
Contact Email : sboochir@cisco.com
Contact Phone :
Street Address :
Affected Chassis : Cisco-uBR7246VXR
Affected Chassis Serial Number : SAB044900Q0
Affected Chassis Part No :  00-0000-00
Affected Chassis Hardware Version : 2.0
Supervisor Software Version : 12.2(20100331:225906)
Command Output Name : show diag
Attachment Type : command output
MIME Type : text/plain
```

Sample Inventory Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope
xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session
xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-
```

```
session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M4::CF1DC8D1</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block
xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/inventory</aml-blo
ck:Type>
<aml-block:CreationDate>2010-02-11 00:07:45
GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>C7200 Family</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G5::CF1DC8D1</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch-inv:CallHome
xmlns:ch-inv="http://www.cisco.com/2005/05/callhome/inventory"
version="1.0">
<ch-inv:EventTime>2010-02-11 00:07:41 GMT+00:00</ch-inv:EventTime>
<ch-inv:MessageDescription>Full Inventory</ch-inv:MessageDescription>
<ch-inv:Event>
<ch-inv:Type>inventory</ch-inv:Type>
<ch-inv:SubType>full</ch-inv:SubType>
<ch-inv:Brand>Cisco Systems</ch-inv:Brand>
<ch-inv:Series>Cisco 7200 Series Routers</ch-inv:Series>
</ch-inv:Event>
<ch-inv:CustomerData>
<ch-inv:UserData>
<ch-inv:Email>sboochir@cisco.com</ch-inv:Email>
</ch-inv:UserData>
<ch-inv:ContractData>
<ch-inv:CustomerId></ch-inv:CustomerId>
<ch-inv:SiteId></ch-inv:SiteId>
<ch-inv:ContractId></ch-inv:ContractId>
<ch-inv:DeviceId>@C@</ch-inv:DeviceId>
</ch-inv:ContractData>
<ch-inv:SystemInfo>
<ch-inv:Name>router</ch-inv:Name>
<ch-inv:Contact></ch-inv:Contact>
<ch-inv:ContactEmail>sboochir@cisco.com</ch-inv:ContactEmail>
<ch-inv:ContactPhoneNumber></ch-inv:ContactPhoneNumber>
<ch-inv:StreetAddress></ch-inv:StreetAddress>
</ch-inv:SystemInfo>
<ch-inv:CCOID></ch-inv:CCOID>
</ch-inv:CustomerData>
<ch-inv:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model></rme:Model>
<rme:HardwareVersion>2.0</rme:HardwareVersion>
<rme:SerialNumber></rme:SerialNumber>
<rme:Card>
<rme:Model>PA-4E=</rme:Model>
<rme:SerialNumber>24508052</rme:SerialNumber>
<rme:LocationWithinContainer>1</rme:LocationWithinContainer>
<rme:PartNumber>73-1556-08</rme:PartNumber>
<rme:HardwareVersion>1.14</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
```

```
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>PA-1GE=</rme:Model>
<rme:SerialNumber>18587776</rme:SerialNumber>
<rme:LocationWithinContainer>2</rme:LocationWithinContainer>
<rme:PartNumber>73-3144-03</rme:PartNumber>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>UBR-MC28U</rme:Model>
<rme:SerialNumber>CAT0841006F</rme:SerialNumber>
<rme:LocationWithinContainer>3</rme:LocationWithinContainer>
<rme:PartNumber></rme:PartNumber>
<rme:HardwareVersion>6.5</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>UBR-MC28U</rme:Model>
<rme:SerialNumber>CAT08340U6N</rme:SerialNumber>
<rme:LocationWithinContainer>4</rme:LocationWithinContainer>
<rme:PartNumber></rme:PartNumber>
<rme:HardwareVersion>6.5</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value=" 00-0000-00" />
<rme:AD name="SoftwareVersion" value="12.2(20091219:015541) " />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.271" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 7200
Software (UBR7200-JK9SU2-M), Experimental Version 12.2(20091219:015541)
[sboochir-ubr-latest 269]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 15-Jan-10 15:57 by sboochir" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch-inv:Device>
</ch-inv:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show diag</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Slot 1:
 Ethernet Port adapter, 4 ports
 Port adapter is disabled unsuitable deactivated powered off
 Port adapter insertion time unknown
 EEPROM contents at hardware discovery:
Slot 2:
 Gigabit Ethernet Port adapter, 1 port
 Port adapter is analyzed
 Port adapter insertion time 00:01:04 ago
 EEPROM contents at hardware discovery:
 Hardware revision 1.0          Board revision A1
 Serial number     18587776   Part number    73-3144-03
 FRU Part Number:  PA-1GE=
 Test history      0x0          RMA number     00-00-00
 EEPROM format version 1
 EEPROM contents (hex):
   0x20: 01 98 01 00 01 1B A0 80 49 0C 48 03 00 00 00 00
   0x30: 51 02 73 00 00 00 00 00 00 01 FF FF FF FF FF FF
Slot 3:
 DOCSIS Modem Card (Universal) 2 Down/8 Up (F-connector) with
Integrated Up-converter Port adapter, 2 ports
 Port adapter is analyzed
```

```
Port adapter insertion time 00:01:04 ago
EEPROM contents at hardware discovery:
Controller Type          : 1053
Hardware Revision        : 6.5
Version Identifier (VID) : V01
Top Assy. Part Number    : 800-17733-04
Board Revision           : A0
Product Identifier (PID) : UBR-MC28U
CLEI Code                : IPUIAF2RAB
Deviation Number         : 0-0
Fab Version              : 06
PCB Serial Number        : CAT0841006F
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 04 1D 41 06 05 89 56 30 31 20 C0 46 03
  0x10: 20 00 45 45 04 42 41 30 CB 89 55 42 52 2D 4D 43
  0x20: 32 38 55 C6 8A 49 50 55 49 41 46 32 52 41 42 80
  0x30: 00 00 00 00 02 06 C1 8B 43 41 54 30 38 34 31 30
  0x40: 30 36 46 03 00 81 00 00 00 00 04 00 FF FF FF FF
  0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x90: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xA0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF B9 1D
Calibration Data
      US calibration ID  : 0x5553
      calibration date   : 20041007
      H/W version        : 6.5
      Number of US points: 8
      Number of freqs    : 3

      ------ NA data ------
                          measured gain
      US  freq(kHz)       0db        2db        4db        8db
16db
       0     5000     28.3000    26.4440    24.0820    19.7360
10.3904
       1     5000     28.3000    26.4440    24.0820    19.7360
10.4262
       2     5000     28.3000    26.4440    24.0820    19.4748
10.3700
       3     5000     28.3000    26.4440    24.0820    19.7377
10.4714
       4     5000     28.3000    26.0539    24.0820    19.4693
10.3700
       5     5000     28.3000    26.4440    24.0820    19.7360
10.3956
       6     5000     28.3000    26.4440    24.0820    19.7360
10.3904
       7     5000     28.3000    26.4440    24.0820    19.7360
10.4817
                          measured gain
      US  freq(kHz)       0db        2db        4db        8db
16db
       0    24000     28.9440    27.1336    25.1060    20.0496
11.3960
       1    24000     28.9440    27.2340    25.1060    20.1656
11.3916
       2    24000     28.9440    26.8480    25.1060    20.0000
11.3640
       3    24000     28.9440    27.2340    25.1060    20.8280
12.2560
       4    24000     28.9440    26.8480    25.1060    20.0165
11.3686
```

```
        5    24000     28.9440    27.2340    25.1060    20.8280
11.6802
        6    24000     28.9440    26.8634    25.1060    20.0165
11.3824
        7    24000     28.9440    27.2340    25.1060    20.8280
11.5947
                         measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    42000     28.6017    26.4440    24.6080    20.0000
11.3640
        1    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        2    42000     28.3000    26.4440    24.0820    19.7817
11.3640
        3    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        4    42000     28.3000    26.4440    24.0925    20.0000
11.3640
        5    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        6    42000     28.6214    26.4520    24.6080    20.0000
11.3640
        7    42000     28.6280    26.8480    24.6080    20.0000
11.3640

       ------ EU data ------
                         measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        1     5000     28.6280    26.4440    24.0925    20.0000
11.3640
        2     5000     28.6280    26.4440    24.0820    19.7360
10.4210
        3     5000     28.6280    26.4440    24.0820    20.0000
11.3640
        4     5000     28.3000    26.4440    24.0820    19.7360
10.4108
        5     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        6     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        7     5000     28.6280    26.4440    24.1030    20.0000
11.3640
                         measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        1    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        2    30000     28.9440    27.2340    25.1060    20.8280
12.2560
        3    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        4    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        5    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        6    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        7    30000     29.2480    27.6040    25.1530    20.8280
12.2560
                         measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        1    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        2    65000     28.6280    26.4440    24.0820    19.7360
```

```
10.3854
        3    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        4    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        5    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        6    65000     28.9440    26.8480    24.1977    19.7483
11.3640
        7    65000     29.2480    26.9406    24.6080    20.0000
11.3640
Slot 4:
 DOCSIS Modem Card (Universal) 2 Down/8 Up (F-connector) with
Integrated Up-converter Port adapter, 2 ports
 Port adapter is analyzed
 Port adapter insertion time 00:01:05 ago
 EEPROM contents at hardware discovery:
 Controller Type          : 1053
 Hardware Revision        : 6.5
 Version Identifier (VID) : V01
 Top Assy. Part Number    : 800-17733-04
 Board Revision           : A0
 Product Identifier (PID) : UBR-MC28U
 CLEI Code                : IPUIAF2RAB
 Deviation Number         : 0-0
 Fab Version              : 06
 PCB Serial Number        : CAT08340U6N
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 04 1D 41 06 05 89 56 30 31 20 C0 46 03
   0x10: 20 00 45 45 04 42 41 30 CB 89 55 42 52 2D 4D 43
   0x20: 32 38 55 C6 8A 49 50 55 49 41 46 32 52 41 42 80
   0x30: 00 00 00 00 02 06 C1 8B 43 41 54 30 38 33 34 30
   0x40: 55 36 4E 03 00 81 00 00 00 00 04 00 FF FF FF FF
   0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x90: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xA0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF E9 1C
 Calibration Data
       US calibration ID  : 0x5553
       calibration date   : 20040824
       H/W version        : 6.5
       Number of US points: 8
       Number of freqs    : 3

       ------ NA data ------
                          measured gain
       US  freq(kHz)       0db        2db        4db        8db
16db
        0     5000     27.9580    26.0200    23.5220    19.3700
10.3700
        1     5000     27.9580    26.0200    24.0820    19.4362
10.3854
        2     5000     27.9580    26.0200    24.0820    19.4178
10.3700
        3     5000     27.9580    26.0200    23.5220    19.3865
10.3700
        4     5000     27.9580    26.0200    23.5220    19.3920
10.3700
        5     5000     27.9580    26.0200    23.5220    19.3718
10.3700
        6     5000     27.9580    26.0200    23.5220    19.3057
10.3700
```

```
        7     5000     28.3000    26.4440    24.0820    19.4436
10.3700
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    24000     28.9440    27.2340    25.1060    20.1656
11.3778
        1    24000     29.2480    27.2340    25.1060    20.8280
12.2560
        2    24000     29.2419    27.2340    25.1060    20.8280
12.2560
        3    24000     28.9440    27.2340    25.1060    20.7783
11.3916
        4    24000     28.9440    27.2340    25.1060    20.0496
11.3732
        5    24000     28.9440    27.2340    25.1060    20.0331
11.3686
        6    24000     28.9440    26.8480    24.6080    20.0000
11.3640
        7    24000     29.2480    27.6040    25.1060    20.8280
12.2560
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    42000     28.9440    27.2340    25.1060    20.8280
12.2560
        1    42000     29.2480    27.6040    25.1060    20.8280
12.2560
        2    42000     29.2480    27.6040    25.1530    20.8280
12.2560
        3    42000     29.2480    27.6040    25.1060    20.8280
12.2560
        4    42000     28.9440    27.2340    25.1060    20.8280
12.0096
        5    42000     28.9440    27.2340    25.1060    20.8280
11.4640
        6    42000     28.9440    27.2340    25.1060    20.1324
11.3732
        7    42000     29.5126    27.6040    25.5760    20.8280
12.2560

       ------ EU data ------
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        1     5000     28.9440    27.2340    25.1060    20.0165
11.4326
        2     5000     28.9440    26.8634    25.1060    20.0000
11.3686
        3     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        4     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        5     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        6     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        7     5000     29.2480    27.2340    25.1060    20.0331
11.3686
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    30000     28.9440    27.2340    25.1060    20.8280
11.4233
        1    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        2    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        3    30000     28.9440    27.2340    25.1060    20.8280
11.4188
        4    30000     28.9440    27.2340    25.1060    20.3808
```

```
11.4006
        5    30000     28.9440    27.2340    25.1060    20.3974
11.3778
        6    30000     28.9440    26.8480    25.1060    20.0000
11.3686
        7    30000     29.2480    27.6040    25.1060    20.8280
12.2560
                         measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    65000     29.2480    27.2340    25.1060    20.2318
11.3732
        1    65000     29.5420    27.6040    25.1060    20.8280
12.2560
        2    65000     29.2480    27.2340    25.1060    20.0496
11.3732
        3    65000     29.2480    27.2340    25.1060    20.0331
11.3686
        4    65000     29.2419    27.2340    24.6378    20.0000
11.3640
        5    65000     29.2480    26.9406    24.6080    20.0000
11.3640
        6    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        7    65000     29.5420    27.6040    25.1060    20.8280
12.2560
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show version</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Cisco IOS Software, 7200 Software (UBR7200-JK9SU2-M),
Experimental Version 12.2(20091219:015541) [sboochir-ubr-latest 269]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 15-Jan-10 15:57 by uname
ROM: System Bootstrap, Version 12.3(4r)T1, RELEASE SOFTWARE (fc1)
 router uptime is 1 minute
System returned to ROM by reload at 23:55:23 UTC Wed Feb 10 2010
System image file is "disk2:ubr7200-jk9su2-mz"
Last reload type: Normal Reload
Last reload reason: Reload command
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
cisco uBR7246VXR (UBR7200-NPE-G1) processor (revision A) with 229376K/32768K bytes of memory.
Processor board ID SAB044900Q0
SB-1 CPU at 700Mhz, Implementation 0x401, Rev 0.2, 512KB L2 Cache
6 slot VXR midplane, Version 2.0
Last reset from power-on
PCI bus mb1 has 74 bandwidth points
PCI bus mb2 has 474 bandwidth points
4 Gigabit Ethernet interfaces
4 Cable Modem interfaces
509K bytes of non-volatile configuration memory.
1992816K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
16384K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory oid</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[NAME: "Chassis", DESCR: "uBR7246VXR Universal Broadband Router"
PID: UBR7246VXR        , VID: N/A, SN: SAB044900Q0
OID: 1.3.6.1.4.1.9.12.3.1.3.134
NAME: "UBR7200-NPE-G1 0", DESCR: "Cisco 7200 Series Network Processing
```

```
Engine NPE-G1"
PID: UBR7200-NPE-G1    , VID:    , SN: 31689947
OID: 1.3.6.1.4.1.9.12.3.1.9.5.56
NAME: "disk2", DESCR: "Compact Flash Disk for NPE-G1"
PID: Unknown Compact Flash, VID:    , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.2.120
NAME: "module 2", DESCR: "GigabitEthernet"
PID: PA-1GE=           , VID: N/A, SN: 18587776
OID: 1.3.6.1.4.1.9.12.3.1.9.4.59
NAME: "module 3", DESCR: "MC28U_F_connector"
PID: UBR-MC28U         , VID: V01 , SN: CAT0841006F
OID: 1.3.6.1.4.1.9.12.3.1.9.27.34
NAME: "module 4", DESCR: "MC28U_F_connector"
PID: UBR-MC28U         , VID: V01 , SN: CAT08340U6N
OID: 1.3.6.1.4.1.9.12.3.1.9.27.34
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show environment all</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Power Supplies:
 Power Supply 1 is unmeasured.
 Power Supply 2 is unmeasured.
Temperature readings:
 NPE Inlet        measured at 34C/93F
 NPE Outlet       measured at 39C/102F
 chassis outlet 3 measured at 29C/84F
 chassis outlet 4 measured at 32C/89F
Voltage readings:
 +3.5 V           measured at +3.43 V
 +5.2 V           is unmeasured
 +12.2 V          is unmeasured
 -12.2 V          is unmeasured
 +16 V            is unmeasured
 -16 V            is unmeasured
Fans:
 Still warming up. Fan deltas not available.
Envm stats saved 0 time(s) since reload
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show c7200</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=4000, netint mask usec=400
uBR7200 Midplane EEPROM:
 Controller Type          : 374
 Number of Slots          : 6
 Hardware Revision        : 1.5
 Top Assy. Part Number    : 800-05443-03
 Board Revision           : A0
 Deviation Number         : 0-0
 Fab Version              : 03
 PCB Serial Number        : SDA05020652
 Chassis Serial Number    : SAB044900Q0
 Chassis MAC Address      : 0004.9bef.3400
 MAC Address block size   : 1024
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 01 76 01 06 41 01 05 C0 46 03 20 00 15
   0x10: 43 03 42 41 30 80 00 00 00 00 02 03 C1 8B 53 44
   0x20: 41 30 35 30 32 30 36 35 32 C2 8B 53 41 42 30 34
   0x30: 34 39 30 30 51 30 C3 06 00 04 9B EF 34 00 43 04
   0x40: 00 03 00 81 00 00 00 00 04 00 C7 20 45 53 00 45
   0x50: 00 50 00 40 00 44 00 3A 00 40 00 7F 00 7E 00 7F
   0x60: 00 84 00 88 00 BC A8 21 00 00 B8 9A FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
uBRuBR7246VXR CPU EEPROM:
 Controller Type          : 859
 Hardware Revision        : 1.4
 Top Assy. Part Number    : 800-22164-05
 CLEI Code                : CNSP30ZAAB
 PCB Part Number          : 73-6988-10
 Board Revision           : A0
 PCB Serial Number        : 31689947
 RMA History              : 00
 Fab Version              : 05
 Fab Part Number          : 28-5082-05
 Product Identifier (PID) : UBR7200-NPE-G1
 Deviation Number         : 0-0
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 03 5B 41 01 04 C0 46 03 20 00 56 94 05
   0x10: C6 8A 43 4E 53 50 33 30 5A 41 41 42 82 49 1B 4C
   0x20: 0A 42 41 30 C1 8B 33 31 36 38 39 39 34 37 00 00
   0x30: 00 04 00 02 05 85 1C 13 DA 05 CB 8E 55 42 52 37
   0x40: 32 30 30 2D 4E 50 45 2D 47 31 80 00 00 00 00 FF
   0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
TLB entries (43/64 used):
Virt Address range      Phy Address range         Attributes
0x4B000000:0x4B1FFFFF   0x14B000000:0x14B1FFFFF   CacheMode=2, RW,
Invalid
0x4B200000:0x4B3FFFFF   0x14B200000:0x14B3FFFFF   CacheMode=2, RW,
Invalid
0x10000000:0x10001FFF   0x0FC010000:0x0FC011FFF   CacheMode=2, RW, Valid
0x42000000:0x43FFFFFF   0x062000000:0x063FFFFFF   CacheMode=2, RW, Valid
0x46000000:0x47FFFFFF   0x066000000:0x067FFFFFF   CacheMode=2, RW, Valid
0x3C000000:0x3C7FFFFF   0x068000000:0x0687FFFFF   CacheMode=2, RW,
Invalid
0x04000000:0x05FFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x08000000:0x09FFFFFF   0x076000000:0x077FFFFFF   CacheMode=2, RW, Valid
0x30000000:0x31FFFFFF   0x06C000000:0x06DFFFFFF   CacheMode=2, RW, Valid
0x38000000:0x39FFFFFF   0x078000000:0x079FFFFFF   CacheMode=2, RW, Valid
0x34000000:0x35FFFFFF   0x070000000:0x071FFFFFF   CacheMode=2, RW,
Invalid
0x4C000000:0x4DFFFFFF   0x07C000000:0x07DFFFFFF   CacheMode=2, RW,
Invalid
0x1FC00000:0x1FC7FFFF   0x01FC00000:0x01FC7FFFF   CacheMode=2, RO, Valid
0x1E000000:0x1E7FFFFF   0x01E000000:0x01E7FFFFF   CacheMode=2, RW, Valid
0x1E800000:0x1E9FFFFF   0x01E800000:0x01E9FFFFF   CacheMode=2, RW, Valid
0x32000000:0x33FFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x3A000000:0x3BFFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x36000000:0x37FFFFFF   0x052000000:0x053FFFFFF   CacheMode=2, RW,
Invalid
0x4E000000:0x4FFFFFFF   0x05E000000:0x05FFFFFFF   CacheMode=2, RW,
Invalid
0x60000000:0x61FFFFFF   0x000000000:0x001FFFFFF   CacheMode=5, RO, Valid
0x62000000:0x627FFFFF   0x002000000:0x0027FFFFF   CacheMode=5, RO, Valid
0x62800000:0x62FFFFFF   0x002800000:0x002FFFFFF   CacheMode=5, RO, Valid
0x63000000:0x631FFFFF   0x003000000:0x0031FFFFF   CacheMode=5, RO, Valid
0x63200000:0x6321FFFF   0x003200000:0x00321FFFF   CacheMode=5, RO, Valid
0x63220000:0x63227FFF   0x003220000:0x003227FFF   CacheMode=5, RO, Valid
0x63228000:0x6322FFFF   0x003228000:0x00322FFFF   CacheMode=5, RO, Valid
0x63230000:0x63231FFF   0x003230000:0x003231FFF   CacheMode=5, RO, Valid
0x63232000:0x63233FFF   0x003232000:0x003233FFF   CacheMode=5, RO, Valid
0x63234000:0x63235FFF   0x003234000:0x003235FFF   CacheMode=5, RO, Valid
0x63236000:0x63237FFF   0x003236000:0x003237FFF   CacheMode=5, RW, Valid
0x63238000:0x6323FFFF   0x003238000:0x00323FFFF   CacheMode=5, RW, Valid
0x63240000:0x6325FFFF   0x003240000:0x00325FFFF   CacheMode=5, RW, Valid
0x63260000:0x6327FFFF   0x003260000:0x00327FFFF   CacheMode=5, RW, Valid
0x63280000:0x632FFFFF   0x003280000:0x0032FFFFF   CacheMode=5, RW, Valid
0x63300000:0x6337FFFF   0x003300000:0x00337FFFF   CacheMode=5, RW, Valid
0x63380000:0x633FFFFF   0x003380000:0x0033FFFFF   CacheMode=5, RW, Valid
0x63400000:0x635FFFFF   0x003400000:0x0035FFFFF   CacheMode=5, RW, Valid
0x63600000:0x637FFFFF   0x003600000:0x0037FFFFF   CacheMode=5, RW, Valid
```

```
0x63800000:0x63FFFFFF   0x003800000:0x003FFFFFF   CacheMode=5, RW, Valid
0x64000000:0x65FFFFFF   0x004000000:0x005FFFFFF   CacheMode=5, RW, Valid
0x66000000:0x67FFFFFF   0x006000000:0x007FFFFFF   CacheMode=5, RW, Valid
0x68000000:0x6FFFFFFF   0x008000000:0x00FFFFFFF   CacheMode=5, RW, Valid
0x0E000000:0x0FFFFFFF   0x00E000000:0x00FFFFFFF   CacheMode=5, RW, Valid
System was restarted by reload at 23:55:23 UTC Wed Feb 10 2010
7200 Software (UBR7200-JK9SU2-M), Experimental Version
12.2(20091219:015541) [sboochir-ubr-latest 269]
Compiled Fri 15-Jan-10 15:57 by sboochir
Image text-base: 0x600092A4, data-base: 0x63243750
Current trace buffer contents:
FP: 0x68213ED0, RA: 0x60D29754
FP: 0x68213ED0, RA: 0x60D0F6EC
FP: 0x68213EE8, RA: 0x60D2F5D8
FP: 0x68213F00, RA: 0x60D33308
FP: 0x68213F48, RA: 0x60B750D0
FP: 0x68214078, RA: 0x60B475EC
FP: 0x68214100, RA: 0x60B731D0
FP: 0x68214198, RA: 0x60CBB68C
0 spurious cache errors detected.
System Controller Network Interrupts
 Wrapper is INSTALLED at address 0x60DF299C
 Interrupt Register is at 0xB0020040 (0x0000000000000000)
Registered Interrupts:
 Level Mask               Count      Data       Interrupt Handler
 0     0x0000000000200000 20         0x69486110 0x6017123C
(GigabitEthernet0/3)
 0     0x0000000000100000 0          0x69470C08 0x6017123C
(GigabitEthernet0/2)
 0     0x0000000000080000 82         0x6945AAC4 0x6017123C
(GigabitEthernet0/1)
 1     0x0000000800000000 2          0x00000000 0x60171888 (SBETH media
interrupt)
 1     0x0000000000001000 6          0x00000000 0x60DF2514 (BCM-1250
PCMCIA)
 2     0x0000000000000020 0          0x6831E720 0x60DF2DD0 (SB1250 Timer
3)
 2     0x0000000000000010 0          0x6831E658 0x60DF2DD0 (SB1250 Timer
2)
 2     0x0000000000000008 0          0x6831E590 0x60DF2DD0 (SB1250 Timer
1)
 2     0x0000000000000004 0          0x6831E4C8 0x60DF2DD0 (SB1250 Timer
0)
 4     0x007C00000000E0C3 0          0x00000000 0x60DFD240 (Spurious
Intr ERROR Handler)
 4     0x0000000000020000 0          0x00000000 0x60DFCD50 (Corrected
ECC Error Handler)
 4     0x0000000000010000 0          0x00000000 0x60DFC98C (Bad ECC
Error Handler)
 4     0x0000003000000000 0          0x00000000 0x60DF2530 (Sturgeon
Error Handler)
 4     0x0003000000000000 0          0x66A227C8 0x60DFCDD8 (BCM1250 Host
LDT Bridge Error Handler)
 4     0x0000000000040000 0          0x00000000 0x60DFD094 (BCM1250
IO-Bus Error Handler)
 4     0x0080000000000000 0          0x00000000 0x60DFCE60 (BCM1250 Host
PCI Bridge Error Handler)
router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Sample Syslog Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
```

```
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MDA:SPE100202ZH:D0600862</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2010-10-13 10:28:50 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>uBR10000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GDB:SPE100202ZH:D0600862</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:28:37 GMT+00:00</ch:EventTime>
<ch:MessageDescription>SLOT 8/1: Oct 13 10:28:36.658: %LICENSE-6-INSTALL: Feature US_License
 1.0 was installed in this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=0:Primary License
 Storage</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>UBR10012</rme:Model>
<rme:HardwareVersion>257</rme:HardwareVersion>
<rme:SerialNumber>SPE100202ZH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-09026-03" />
<rme:AD name="SoftwareVersion" value="12.2(20100929:171810)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.317" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M),
 Experimental Version 12.2(20100929:171810) [pauhuang-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by pauhuang" />
</rme:AdditionalInformation>
```

```
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 15 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: level debugging, 4756 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 6755 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
    Trap logging: level informational, 6388 message lines logged
Log Buffer (12800000 bytes):
*Oct 11 03:42:07.367: CM file (ivfs:/ubr10k4-k9p6u2-m_matrix.cm) is not readable, using
internal matrix table
*Oct 11 03:42:08.799: %C10K_TOASTER-6-STARTLOAD: Downloading Microcode:
file=system:pxf/c10k-cr4-ucode.101.0.0.0, version=101.0.0.0, description=Nightly Build
Software created Mon 27-Sep-10 16:12
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed
 state to up
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to up
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Oct 11 03:42:10.447: %LINK-3-UPDOWN: Interface FastEthernet0/0/0, changed state to up
*Oct 11 03:42:10.691: %RED-5-REDCHANGE: PRE B now Non-participant(0x0 => 0x1421)
*Oct 11 03:42:11.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/0,
changed state to down
*Oct 11 03:42:11.639: %IPCOIR-5-IVFS_FILE_LOADING: Extracting 5cable-mc520u-d from
ivfs:/ubr10kclc-lck8-mz.card.
*Oct 11 03:42:12.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/0,
 changed state to down
...
...
...
Modular-Cable1/1/0:0, changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:1,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:2,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:3,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:4,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
...
...
...
GigabitEthernet3/1/0, changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/0/0,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/0, changed
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/0 changed state to
down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/1, changed
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/1 changed state to
down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/2, changed
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/2 changed state to
```

```
down
tate to up
*Oct 11 03:42:22.491: %UBR10000-5-UPDOWN: Interface Cable5/1/3 U0, changed state to down
*Oct 11 03:42:22.495: %UBR10000-5-USFREQCHG: Interface Cable5/1/3 U0, changed to Freq 25.000
 MHz
*Oct 11 03:42:22.503: %UBR10000-5-UPDOWN: Interface Cable5/1/3 U1, changed state to down
*Oct 11 03:42:22.507: %UBR10000-5-USFREQCHG: Interface Cable5/1/3 U1, changed to Freq 26.600
 MHz
*Oct 11 03:42:23.911: %UBR10000-5-USFREQCHG: Interface Cable7/1/2 U0.1, changed to Freq
10.000 MHz
*Oct 11 03:42:23.911: %UBR10000-5-USFREQCHG: Interface Cable7/1/2 U0.1, changed to Freq
10.000 MHz
*Oct 11 03:42:23.911: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U0.1, changed state to down
*Oct 11 03:42:23.923: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U1, changed state to down
*Oct 11 03:42:23.935: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U2, changed state to down
*Oct 11 03:42:23.947: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U3, changed state to down
*Oct 11 03:42:23.951: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U3.1, changed state to down
...
...
...
*Oct 11 03:42:25.795: %LINK-3-UPDOWN: Interface Cable6/1/3, changed state to down
*Oct 11 03:42:25.795: %LINK-3-UPDOWN: Interface Cable6/1/4, changed state to down
*Oct 11 03:42:25.795: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U0, changed state to down
*Oct 11 03:42:25.807: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U1, changed state to down
*Oct 11 03:42:25.819: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U2, changed state to down
*Oct 11 03:42:25.831: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U3, changed state to down
...
...
...
*Oct 11 03:42:30.175: %IPCOIR-3-CARD_UNSUPPORTED: Unsupported card type (0x415) in slot
1/0.
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_DETECTED: Card type 2jacket-1 (0x415) in slot 1/0
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_LOADING: Loading card in slot 4/0 sw version 4.0 code
 MD5 FFE6204BD2DED9385026C375D457564A fpga MD5 E5099933C1DDD6B76260A6085BD1CDDF
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_LOADING: Loading card in slot 1/0 sw version 1.1 code
 MD5 3716BEAEB613954FB02A236E6636B299 fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:30.179: %IPCOIR-5-CARD_DETECTED: Card type 2cable-dtcc (0x5B0) in slot 2/1
*Oct 11 03:42:30.183: %IPCOIR-5-CARD_LOADING: Loading card in slot 2/1 sw version 1.0 code
 MD5 08BB3163BD9E82D61F2A78200397187D fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:30.775: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [pauhuang-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by pauhuang
*Oct 11 03:42:30.791: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 03:42:30.795: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:31.115: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle1, changed state
 to up
*Oct 11 03:42:31.119: %SNMP-5-LINK_UP: LinkUp:Interface Bundle1 changed state to up
*Oct 11 03:42:31.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle2, changed state
 to up
*Oct 11 03:42:31.123: %SNMP-5-LINK_UP: LinkUp:Interface Bundle2 changed state to up
*Oct 11 03:42:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle3, changed state
 to up
*Oct 11 03:42:31.127: %SNMP-5-LINK_UP: LinkUp:Interface Bundle3 changed state to up
*Oct 11 03:42:31.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle4, changed state
 to up
*Oct 11 03:42:31.131: %SNMP-5-LINK_UP: LinkUp:Interface Bundle4 changed state to up
*Oct 11 03:42:31.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/0,
changed state to up
*Oct 11 03:42:31.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle60, changed
state to up
*Oct 11 03:42:31.135: %SNMP-5-LINK_UP: LinkUp:Interface Bundle60 changed state to up
*Oct 11 03:42:31.503: %SYS-6-BOOTTIME: Time taken to reboot after reload = 423551 seconds
*Oct 11 03:42:32.523: %LINK-3-UPDOWN: Interface HTDP0/0/1, changed state to up
*Oct 11 03:42:32.783: %C10K-5-LC_NOTICE: Slot[4/0] Line-card Image Downloaded...Booting...
*Oct 11 03:42:33.523: %LINEPROTO-5-UPDOWN: Line protocol on Interface HTDP0/0/1, changed
state to up
*Oct 11 03:42:35.555: %C10K_TOASTER-6-STARTPXF:
!!pxf clients started, forwarding code operational!!
*Oct 11 03:42:35.951: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-5x20s (0x348) in slot
```

```
6/1
*Oct 11 03:42:36.007: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1 sw version 1.0 code
 MD5 33AD44802F7069858C7A18315833494D fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:36.359: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-5x20s (0x348) in slot
5/0
...
...
...
*Oct 11 03:44:09.923: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/1/4 changed state to up
*Oct 11 03:45:40.751: cr10k_clnt_issu_start_nego_session at slot 8/0 clnt 0:rp-lc:rp-lc ses
 131081 nego Yes ISSU/my compat Yes/Yes
*Oct 11 03:45:41.823: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 03:45:41.823: CR10K DOCSIS C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K HCCP C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K PKTCBL C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K PLFM C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K SNMP C8/0 is up for apps
*Oct 11 03:45:41.831: CR10K GUARDIAN C8/0 is up for apps
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 0 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U0, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 1 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U1, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 2 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U2, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 3 has been shutdown
 due to insufficient licenses
...
...
...
*Oct 11 04:08:41.287: %CMTS_LIC-6-CHANNEL_NO_SHUTDOWN: Cable8/0/3 channel 0 has been restored
 to no shut
*Oct 11 04:08:41.287: %CMTS_LIC-6-OUT_OF_RANGE: LC 8/0, Forced Shut US License Count is
already 0
-Traceback= 40ACB68C 401C7694 401C77E4 401C71F8 401AC3CC 40258AA8 401C7A94 401C7FCC 401C8140
 401C9288 401C94D0 401AE5BC 40CEFD3C 40CFD49C 40A50BAC 40150EC8
*Oct 11 04:08:41.291: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U0, changed state to down
*Oct 11 04:08:41.291: %CMTS_LIC-6-CHANNEL_NO_SHUTDOWN: Cable8/0/3 channel 1 has been restored
 to no shut
*Oct 11 04:08:41.291: %CMTS_LIC-6-OUT_OF_RANGE: LC 8/0, Forced Shut US License Count is
already 0
...
...
...
*Oct 11 04:16:14.851: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:18:48.847: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 04:18:48.851: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:21:18.859: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 04:21:18.859: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:29:09.763: %UBR10K-1-POWCYCLE: Power cycle slot 6/0
*Oct 11 04:29:17.931: %LCINFO-4-LCHUNG: Slot [6/0] down on last 11 checks.  HW RESET # 3
...
...
...
*Oct 11 09:05:26.702: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
 changed state to down
*Oct 11 09:05:39.382: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.382: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.382: wbchannel_delete_context Modular-Cable
*Oct 11 09:05:39.582: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.582: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.582: wbchannel_delete_context Modular-Cable
*Oct 11 09:05:39.782: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.782: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.782: wbchannel_delete_context Modular-Cable
```

```
*Oct 11 09:05:39.986: %C10K-3-DEACTIVATED: card in slot [8/0] disabled.
*Oct 11 09:05:47.670: %UBR10000-5-USFREQCHG: Interface Cable8/0/0 U0, changed to Freq 10.000
 MHz
...
...
...
*Oct 11 16:48:26.188: CR10K DOCSIS C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K HCCP C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K PKTCBL C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K PLFM C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K SNMP C8/1 is up for apps
*Oct 11 16:48:26.704: CR10K GUARDIAN C8/1 is up for apps
*Oct 11 16:48:28.068: cr10k_clnt_issu_start_nego_session at slot 8/0 clnt 0:rp-lc:rp-lc ses
 458761 nego Yes ISSU/my compat Yes/Yes
*Oct 11 16:48:28.084: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 16:48:28.084: CR10K DOCSIS C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K HCCP C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K PKTCBL C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K PLFM C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K SNMP C8/0 is up for apps
*Oct 11 16:48:28.092: CR10K GUARDIAN C8/0 is up for apps
*Oct 11 16:48:50.456: CR10K DOCSIS C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K HCCP C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K PKTCBL C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K PLFM C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K SNMP C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K GUARDIAN C8/0 is down for apps
*Oct 11 16:48:50.460: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 8/0.
*Oct 11 16:48:50.460: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is down.  Notifying
ubr10k-clc-3g60 driver.
*Oct 11 16:48:51.456: %C10K-5-SUBSLOT_RESET: Card in slot 8/0 has been reset
*Oct 11 16:49:23.744: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 16:49:23.744: %IPCOIR-5-CARD_LOADING: Loading card in slot 8/0 sw version 1.0 code
 MD5 15247BBB545BF3FAE97D7E7D34C1177C fpga MD5 00000000000000000000000000000000
*Oct 11 16:49:26.708: %CR10K_CLNT-3-TIMEOUT: Timeout waiting for RP-LIC: card license ready,
 slot 8/1
-Traceback= 40ACB68C 40DCA7FC 401AE8E0 40CEDF00 40CF37CC 40BC79DC 40BC79C8
*Oct 11 16:49:28.092: %CR10K_CLNT-3-TIMEOUT: Timeout waiting for RP-LIC: card license ready,
 slot 8/0
...
...
...
*Oct 13 04:12:04.931: cr10k_clnt_issu_receive_nego_message at slot 8/1 clnt 0:rp-lc:rp-lc
ses 1179700 nego Yes ISSU/my compat Yes/Yes
*Oct 13 04:12:05.143: CR10K HCCP C8/1 is up for apps
*Oct 13 04:12:05.203: CR10K GUARDIAN C8/1 is up for apps
*Oct 13 04:12:05.259: CR10K PLFM C8/1 is up for apps
*Oct 13 04:12:05.271: CR10K PKTCBL C8/1 is up for apps
*Oct 13 04:12:05.299: CR10K SNMP C8/1 is up for apps
*Oct 13 04:12:05.795: CR10K DOCSIS C8/1 is up for apps
*Oct 13 04:12:07.739: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 8/0.
*Oct 13 04:12:07.739: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is down.  Notifying
ubr10k-clc-3g60 driver.
*Oct 13 04:12:07.739: %C10K-3-EEPROM_ERROR: c10k_load_slot_eeprom_copy failed on subslot
8/0
-Traceback= 40ACB68C 40CDD418 40CCE018 40CCE2F4 40A50BAC 40150EC8 40A7D068 40BC79DC 40BC79C8
*Oct 13 04:12:07.743: %C10K-3-EEPROM_ERROR: c10k_load_slot_eeprom_copy failed on subslot
8/0
-Traceback= 40ACB68C 40CDD274 40CCE05C 40CCE2F4 40A50BAC 40150EC8 40A7D068 40BC79DC 40BC79C8
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/0, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/1, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/2, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/3, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/4, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/5, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/6, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/7, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/8, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/9, changed state to down
...
...
```

```
...
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/0, changed state to down
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/2, changed state to down
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/4, changed state to down
*Oct 13 05:38:46.815: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 13 05:38:46.839: cr10k_clnt_issu_receive_nego_message at slot 8/0 clnt 0:rp-lc:rp-lc
ses 589887 nego Yes ISSU/my compat Yes/Yes
*Oct 13 05:38:48.095: CR10K HCCP C8/0 is up for apps
*Oct 13 05:38:48.159: CR10K GUARDIAN C8/0 is up for apps
*Oct 13 05:38:48.271: CR10K PLFM C8/0 is up for apps
*Oct 13 05:38:48.283: CR10K PKTCBL C8/0 is up for apps
*Oct 13 05:38:48.311: CR10K SNMP C8/0 is up for apps
*Oct 13 05:38:48.679: CR10K DOCSIS C8/0 is up for apps
*Oct 13 05:38:50.735: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is up.  Notifying
ubr10k-clc-3g60 driver.
*Oct 13 05:38:50.847: %LINK-3-UPDOWN: Interface Cable8/0/0, changed state to up
*Oct 13 05:38:50.851: %LINK-3-UPDOWN: Interface Cable8/0/1, changed state to up
*Oct 13 05:38:50.851: %LINK-3-UPDOWN: Interface Cable8/0/2, changed state to up
...
...
...
*Oct 13 09:39:14.606: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:42:05.710: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:43:31.778: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:46:28.726: %LINK-3-UPDOWN: Interface GigabitEthernet8/0/0, changed state to down
*Oct 13 09:46:29.726: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
 changed state to down
*Oct 13 09:46:32.730: %LINK-3-UPDOWN: Interface GigabitEthernet8/0/0, changed state to up
*Oct 13 09:46:33.730: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
 changed state to up
*Oct 13 10:14:39.302: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 10:27:39.126: %SYS-5-CONFIG_I: Configured from console by console
Oct 13 10:28:35.938: CLC-LIC: cmts_clc_cisl_event_notify_feature_us, 1383: received event
1 notification
Oct 13 10:28:35.938: CLC-LIC: cmts_clc_cisl_event_notify_feature_us, 1404: feature US_License
 license_type 0 notifycount 20 usage_count 0 oldcount 0 newcount 0
Oct 13 10:28:35.938: CLC-LIC:cr10k_clc_cisl_handle_count_change_us: slot 8/1 oldcount 0,
newcount 0
...
...
...
SLOT 8/1: Oct 13 10:28:36.658: %LICENSE-6-INSTALL: Feature US_License 1.0 was installed in
 this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=0:Primary License Storage
SLOT 8/1: Oct 13 10:28:36.662: %LICENSE-6-INSTALL: Feature DS_License 1.0 was installed in
 this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=2:Primary License Storage
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[NAME: "Chassis" DESCR: "uBR10000 chassis"
PID: UBR10012          , VID:    , SN: SPE100202ZH
NAME: "RP A" DESCR: "Performance Routing Engine"
PID: ESR-PRE4          , VID: V03 , SN: CAT1336F051
NAME: "RP A flash card 0" DESCR: "Flash Card"
PID: ESR-PRE-MEM-FD128 , VID:    , SN:
NAME: "RP A flash card 1" DESCR: "Flash Card"
PID: ESR-PRE-CF-1GB    , VID:    , SN:
NAME: "RP B" DESCR: "Performance Routing Engine"
PID: ESR-PRE4          , VID:    , SN:
NAME: "Jacket-Card-Slot 1/0" DESCR: "2 bays I/O slot SPA Interface Processor"
PID: UBR10-2XDS-SIP    , VID: 1.0, SN: CAT112358KV
NAME: "SPA bay 1/1" DESCR: "WIDEBAND DOCSIS SPA"
PID: SPA-24XDS-SFP     , VID: V01, SN: CAT1228E21D
NAME: "SFP 1/1/0" DESCR: "Copper GigE SFP"
PID: SP7041-E          , VID: E   , SN: MTC133100GM
NAME: "module 1/1" DESCR: "2 port utility Clock Card"
PID: UBR10-TCC+-T1     , VID:    , SN:
NAME: "module 2/1" DESCR: "2 port DTI UC"
PID: UBR10-DTCC        , VID: 2.0, SN: CAT1213E19M
NAME: "module 3/1" DESCR: "Half-height Gigabit Ethernet MAC Controller"
PID: ESR-HH-1GE        , VID:    , SN:
```

```
NAME: "module 4/0" DESCR: "Half-height Gigabit Ethernet MAC Controller"
PID: ESR-HH-1GE         , VID: 1.0, SN: CAT09190TTY
NAME: "module 5/0" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20U-D    , VID:     , SN: CAT10110AG6
NAME: "module 5/1" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20S      , VID:     , SN:
NAME: "module 6/0" DESCR: "MC2020H_D_connector"
PID: UBR10-MC20X20H     , VID:     , SN:
NAME: "module 6/1" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20U-D    , VID:     , SN: CAT100614L7
NAME: "module 7/1" DESCR: "MC3GX60V"
PID: UBR10-MC3GX60V     , VID:     , SN:
NAME: "module 8/0" DESCR: "MC3GX60V"
PID: UBR-MC3GX60V       , VID: V01 , SN: CSJ13422931
NAME: "SFP 8/0/0/0" DESCR: "SFP"
PID: SP7041-E           , VID: E   , SN: MTC1331009J
NAME: "module 8/1" DESCR: "MC3GX60V"
PID: UBR-MC3GX60V       , VID: V01 , SN: CSJ13302903
NAME: "power-supply 0" DESCR: "DC Power Entry Module for UBR10012"
PID: UBR10-PWR-DC       , VID:     , SN:
NAME: "power-supply 1" DESCR: "DC Power Entry Module for UBR10012"
PID: UBR10-PWR-DC       , VID:     , SN:
NAME: "fan-tray" DESCR: "BLOWER ASSEMBLY FOR UBR10012"
PID: UBR10-FAN-ASSY     , VID:     , SN:
router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Additional References

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Configuring Call Home for Cisco 7200 Series Routers	http://www.cisco.com/en/US/docs/routers/7200/configuration/feature_guides/callhome_7200.html
Cisco License Call Home	http://www.cisco.com/en/US/docs/ios/csa/configuration/guide/csa_callhome.html

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

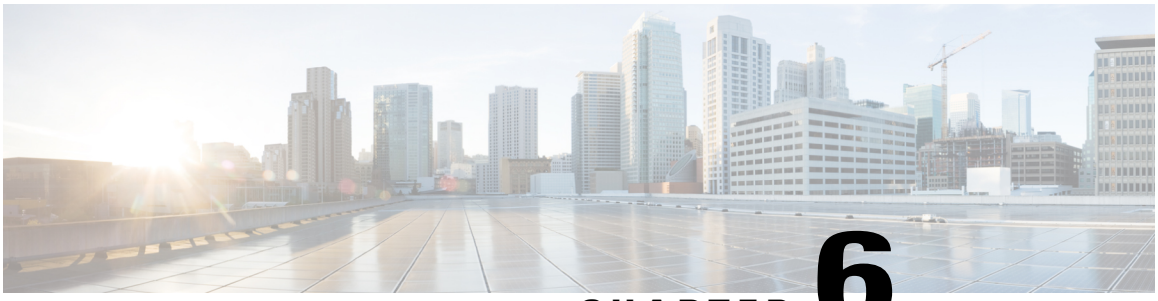
Feature Information for the Call Home Feature for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 4: Feature Information for Call Home Feature for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Call Home Feature for the Cisco CMTS Routers	12.2(33)SCE	This feature was introduced on the Cisco universal broadband routers



CHAPTER 6

Cisco Network Registrar for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

This chapter supplements the Cisco Network Registrar (CNR) documentation by providing additional cable-specific instructions to provision a hybrid fiber-coaxial (HFC) network using Cisco universal broadband routers as CMTSs at the headend of the network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

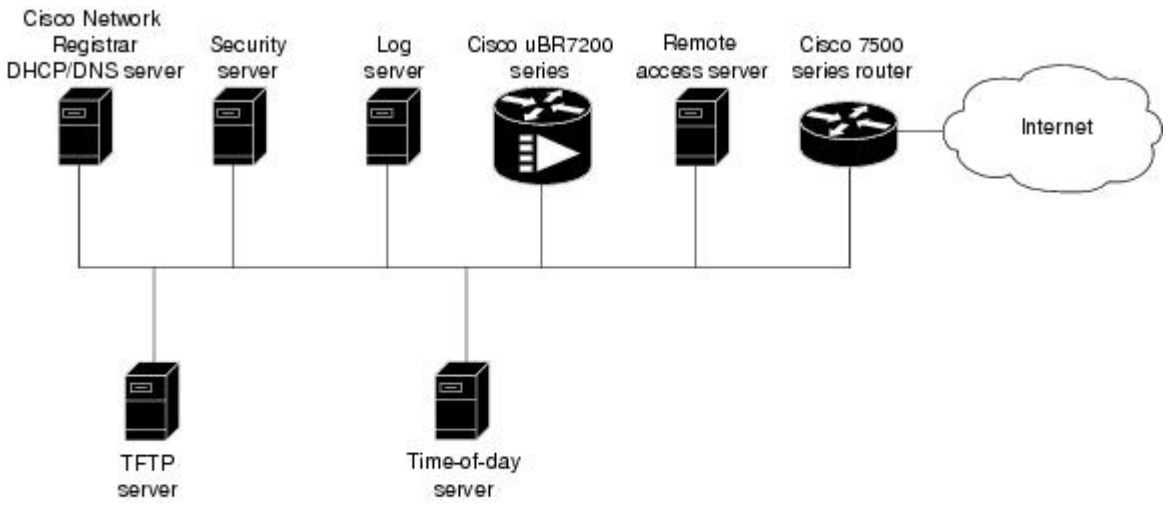
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Servers Required on the HFC Network

A TFTP server, DHCP server, and time-of-day (TOD) server are required to support two-way data cable modems on an HFC network. A cable modem will not boot if these servers are not available. The log server and security servers are not required to configure and operate a cable modem. If the log server or security servers are not present, a cable modem will generate warning messages, but it will continue to boot and function properly.

Figure 1: Servers Required on a Two-Way HFC Network



The servers shown here can exist on the same platform. For example, the time-of-day server and the TFTP server can run on the same platform.

In this provisioning model, TOD and TFTP servers are standard Internet implementations of the RFC 868 and RFC 1350 specifications. Most computers running a UNIX-based operating system supply TOD and TFTP servers as a standard software feature. Typically, the TOD server is embedded in the UNIX *inetd* and it requires no additional configuration. The TFTP server is usually disabled in the standard software but can be enabled by the user. Microsoft NT server software includes a TFTP server that can be enabled with the services control panel. Microsoft NT does not include a TOD server. A public domain version of the TOD server for Microsoft NT can be downloaded from several sites.

The DHCP and Domain Name System (DNS) server shown in Figure above must be the DHCP/DNS server available in Cisco Network Registrar version 2.0 or later. CNR is the only DHCP server that implements

policy-based assignment of IP addresses. The headend must be a Cisco uBR7200 series universal broadband router or Cisco uBR10012 universal broadband router. The remote access server is only required on HFC networks that are limited to one-way (downstream only) communication. In a one-way HFC network, upstream data from a PC through the headend to the Internet is carried over a dialup connection. This dialup connection for upstream data is referred to as telco return. For simplification, the model will not include a log or security server. Cable modems can be set up to use the logging and security servers by including the appropriate DHCP options in the cable modem policy as described in the *Cisco Network Registrar User Manual*.

Cisco Network Registrar Description

CNR is a dynamic IP address management system, running on Windows or Solaris, that uses the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to cable interfaces, PCs, and other devices on the broadband network. The CNR tool includes script extensions that allow a cable system administrator to define and view individual DHCP options, define the identity or type of device on the network, and assign the device to a predefined class or group.

Using the CNR tool, a cable system administrator can specify policies to provide:

- Integrated DHCP and Domain Name Server (DNS) services
- Time of Day (ToD) and Trivial File Transfer Protocol (TFTP) server based on the size of the network
- DHCP safe failover and dynamic DNS updates

Note This is available only in CNR 3.0 or higher.

Using the CNR tool and the extension scripts identified in the Overview of Scripts, on page 126 section, a cable system administrator can specify scopes, policies, and options for the network and each cable interface based on the services and configuration to support at each subscriber site.

Note Scopes refer to the administrative grouping of TCP/IP addresses; all IP addresses within a scope should be on the same subnet.

The cable system administrator defines system default policies for all standard options and uses scope-specific policies for options related to particular subnets, such as cable interfaces. This allows DHCP to send the information with the IP address.

Seven entry points exist for scripts:

- post-packet-decode
- pre-client-lookup
- post-client-lookup—Examines and takes action on results of the client-class process, places data items in the environment dictionary to use at the pre-packet-encode extension point, includes DHCP relay option
- check-lease-acceptable
- pre-packet-encode
- post-sent-packet

- pre-dns-add-forward

Overview of DHCP Using CNR

Cisco Network Registrar (CNR) is a dynamic IP address management system that uses the Dynamic Host Configuration Protocol (DHCP) and assigns IP addresses to PCs and other devices on a network based on a predefined set of policies, such as class of service. CNR assigns available IP addresses from address pools based on the identity or type of the requesting device and the policies in effect. For example, CNR can distinguish between registered devices, unregistered devices, and registered devices that have been assigned to a particular class of service.

CNR also provides extensions that can be customized (via programming or a script) so that you can view individual DHCP options, determine the identity or type of a device based on the content of the options, and assign a device to a predefined class or group. Using these extensions, you can determine the difference between PCs and cable modems and assign them IP addresses from different address pools.

In typical data-over-cable environments, service providers are interested in simplifying provisioning to limit the amount of information that must be collected about subscribers' customer premise equipment (CPEs). To support current provisioning models, a field technician must be sent to a subscriber's home or business to install and setup a cable modem. During this site visit, the technician might register the serial number and MAC address of the cable modem in the customer account database. Because a field technician must go to a subscriber's site to replace a cable modem, you can easily track modem information.

Manually registering and tracking information about a cable subscriber's PC is more difficult. A subscriber might purchase a new PC or exchange the network interface card (NIC) without notifying you of the change. Automatic provisioning with CNR reduces the amount of customer service involvement needed to track customer equipment. To use the provisioning model described in this document, you must still track serial numbers and MAC addresses for cable modems, but you do not need to track information about the PC or NIC cards installed at a subscriber site.

The remainder of this document describes how to configure CNR to support this model. The following sections describe the equipment and servers required for the cable headend, provide an overview of the interaction between DOCSIS-compatible cable modems and the Cisco universal broadband routers, and provide a guide on how to configure CNR to support this provisioning model.

How Cisco Universal Broadband Routers and Cable Modems Work

Cisco universal broadband routers and cable modems are based on the Data Over Cable Service Interface Specification (DOCSIS) standards. These standards were created by a consortium of cable service providers called Multimedia Cable Network Systems, Ltd. (MCNS) to that cable headend and cable modem equipment produced by different vendors will interoperate. The key DOCSIS standards provide the basis for a cable modem to communicate with any headend equipment and headend equipment to communicate with any cable modem.

Cable modems are assigned to operate on specific cable channels so activity can be balanced across several channels. Each Cisco uBR7200 series router installed at the headend serves a specific channel. Part of network planning is to decide which channel each cable modem can use.

A cable modem cannot connect to the network until the following events occur:

- The cable modem initializes and ranges through available frequencies until it finds the first frequency that it can use to communicate to the headend. The cable modem might be another vendor's

DOCSIS-compatible device and the headend might have a Cisco uBR7200 series router installed. At this point on the initial connection, the cable modem cannot determine if it is communicating on the correct channel.

- The cable modem goes through the DHCP server process and receives a configuration file from the server.
- One of the parameters in the configuration file tells the cable modem which channel it can use.
- If the assigned channel is not available on the Cisco uBR7200 series router to which the cable modem is currently connected, it resets itself and comes up on the assigned channel.
- During this second DHCP process, the modem will be connected to the correct CMTS. This time, the configuration file will be loaded. For a DOCSIS-compatible cable modem to access the network, it might go through the DHCP server two times on two different networks; therefore, one-lease-per-client IP addressing is critical.

DHCP Fields and Options for Cable Modems

DHCP options and packet fields are required to enable cable modems to boot and operate properly. Table below lists the required DHCP options and fields.

Table 5: Required DHCP Fields and Options

Required Field/Option	Field/Option In Cisco Network Registrar	Value/Description
Fields		
giaddr	-	IP address. As a DHCP packet passes through the relay agent to the DHCP server, the relay agent supplies a unique IP address to the packet and stores it in this field. The relay agent is a uBR7200 series router with the iphelper attribute defined.
subnet-mask	-	Subnet mask for the IP address stored in the giaddr field. This value is also stored in the DHCP packet by the relay agent.
file	Packet-file-name	Name of the cable modem configuration file that will be read from a TFTP server.
siaddr	Packet-siaddr	IP address of the TFTP server where configuration files are stored.
Options		

Required Field/Option	Field/Option In Cisco Network Registrar	Value/Description
Time-servers	-	List of hosts running the time server specified in the RFC 868 standard.
Time-offset	-	Time offset of a cable modem internal clock from Universal Time Coordinated (UTC). This value is used by cable modems to calculate the local time that is stored in time-stamping error logs.
MCNS-security-server	-	IP address of the security server. This should be set if security is required. See RFC 1533 for details.

Cisco Network Registrar Sample Configuration

You can use the following information to set up Cisco Network Registrar in a trial configuration. The configuration describes DHCP-related setup only; it does not cover setting up DNS or configuring dynamic DNS (DDNS). You should be familiar with important CNR concepts including scopes, primary and secondary scopes, scope selection tags, client classes, and CNR policies. See the Using Network Registrar publication for detailed information on these concepts.

In the trial configuration, you can configure CNR to perform the following operations:

- Receive DHCP requests from a cable modem and a PC on an HFC network via a port supporting multiple network numbers. The Cisco uBR7200 series router at the headend must be configured as a forwarder (iphelper is configured).
- Serve IP addresses on two networks; a net-10 network (non-Internet routable) and a net-24 network (Internet routable).
- Tell the difference between a cable modem and a PC based on the MAC address of the device and provide net-24 addresses to the PC and net-10 addresses to the cable modem.
- Refuse to serve IP addresses to MAC addresses that it does not recognize.

To perform these options, you must implement the following CNR configuration items:

- Create two scope selection tags; one for PCs, one for cable modems.
- Create two client-classes; one for PCs , one for cable modems.
- Create a lease policy appropriate for the cable modem devices.
- Create a lease policy appropriate for the PC devices.
- Create a scope containing Class A net-24 (routable) addresses.
- Create a scope containing Class A net-10 (nonroutable) addresses.

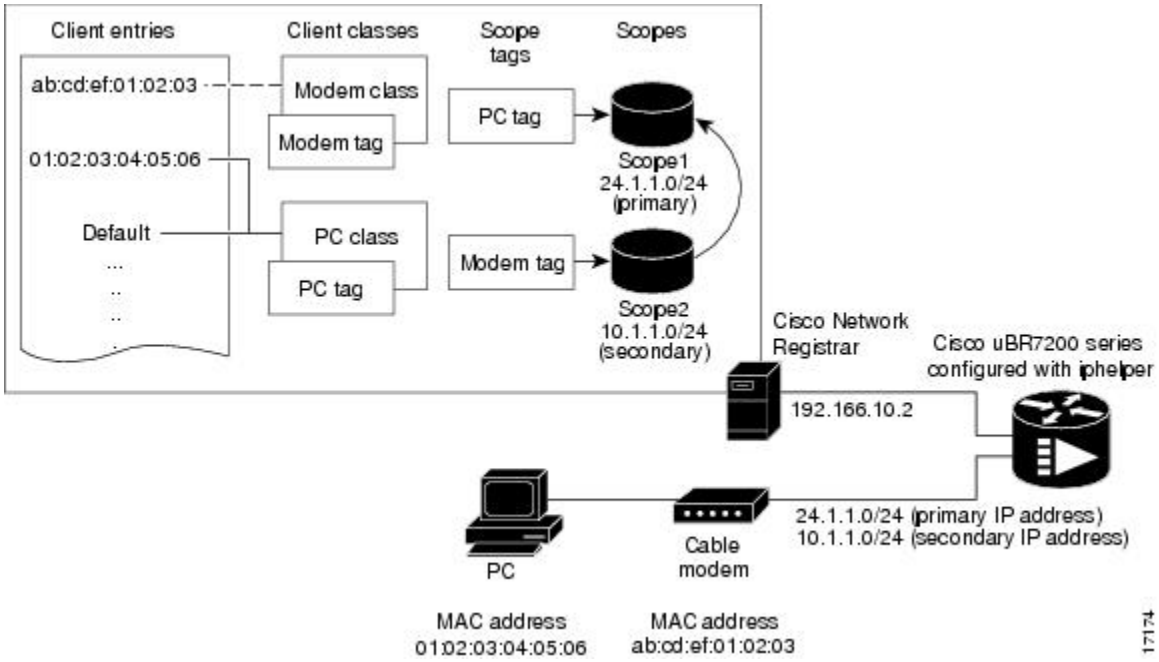
- Identify the scope containing the net-24 addresses as the primary scope and configure the other scope containing the net-10 addresses as secondary to the net-24 scope.

Note The Cisco uBR7200 series router upstream ports must be configured with the primary network address on the net-24 network; such as 24.1.1.1.

- Assign the policies to the appropriate scope.
- Add the MAC address of the cable modem and the PC to the client-entry list.
- Associate the PC tag with the scope containing routable addresses.
- Associate the cable modem tag with the scope containing nonroutable addresses.
- Associate the cable modem tag with the cable modem client-class.
- Associate the PC tag with the PC client-class.
- Assign the PC MAC to the PC class.
- Assign the cable modem MAC to the cable modem class.
- Enable client-class processing.

Figure below shows the trial CNR configuration in an HFC network.

Figure 2: Trial Configuration in an HFC Network



These configuration items and their associations can be created using either the CNR management graphical user interface (GUI) or command-line interface (CLI). The following sample script configures DHCP for a sample server:

```
File: cabledemo.rc
Command line: nrcmd -C <cluster> -N <user name> -P <password> -b < cabledemo.rc
-------------------------------------------------------------------------------
scope-selection-tag tag-CM create
scope-selection-tag tag-PC create
client-class create class-CM
client-class class-CM set selection-criteria=tag-CM
client-class create class-PC
client-class class-PC set selection-criteria=tag-PC
policy cmts-cisco create
policy cmts-cisco setleasetime 1800
policy cmts-cisco setoption domain-name-servers 192.168.10.2
policy cmts-cisco setoption routers 10.1.1.1
policy cmts-cisco setoption time-offset  604800
policy cmts-cisco setoption time-servers 192.168.10.20
policy cmts-cisco set packet-siaddr=192.168.10.2
policy cmts-cisco setoption log-servers 192.168.10.2
policy cmts-cisco setoption mcns-security-server 192.168.10.2
policy cmts-cisco set packet-file-name=golden.cfg
policy cmts-cisco set dhcp-reply-options=packet-file-name,packet-siaddr,mcns-security-server
policy pPC create
policy pPC set server-lease-time 1800
policy pPC setleasetime 1800
policy pPC setoption domain-name-servers 192.168.10.2
policy pPC setoption routers 24.1.1.1
scope S24.1.1.0 create 24.1.1.0 255.255.255.0
scope S24.1.1.0 addrange 24.1.1.5 24.1.1.254
scope S24.1.1.0 set policy=pPC
scope S24.1.1.0 set selection-tags=tag-PC
scope S10.1.1.0 create 10.1.1.0 255.255.255.0
scope S10.1.1.0 addrange 10.1.1.5 10.1.1.254
scope S10.1.1.0 set policy=cmts-cisco
scope S10.1.1.0 set selection-tags=tag-CM
scope S10.1.1.0 set primary-scope=S24.1.1.0
client 01:02:03:04:05:06 create client-class-name=class-PC
client ab:cd:ef:01:02:03 create client-class-name=class-CM
client default create action=exclude
dhcp enable client-class
dhcp enable one-lease-per-client
save
dhcp reload
```

In addition to the DHCP server setup, you might want to enable packet-tracing. When packet-tracing is enabled, the server parses both requests and replies, and then adds them to the logs. If you do enable tracing, performance will be adversely affected, and the logs will roll over quickly.

Use the following nrcmd command to set packet tracing.

DHCP set log-settings=incoming-packet-detail,outgoing-packet-detail

Cable Modem DHCP Response Fields

Each cable interface on the broadband network requires the following fields in the DHCP response:

- CM's IP address
- CM's subnet mask

Note For cable operators with less experience in networking, you can fill in a guess based on the network number and indicate how your IP network is divided.

- Name of the DOCSIS configuration file on the TFTP server intended for the cable interface
- Time offset of the cable interface from the Universal Coordinated Time (UTC), which the cable interface uses to calculate the local time when time-stamping error logs
- Time server address from which the cable interface obtains the current time

DOCSIS DHCP Fields

DOCSIS DHCP option requirements include:

- IP address of the next server to use in the TFTP bootstrap process; this is returned in the siaddr field
- DOCSIS configuration file that the cable interface downloads from the TFTP server

Note If the DHCP server is on a different network that uses a relay agent, then the relay agent must set the gateway address field of the DHCP response.

- IP address of the security server should be set if security is required

DHCP Relay Option (DOCSIS Option 82)

DOCSIS Option82 modifies DHCPDISCOVER packets to distinguish cable interfaces from the CPE devices or “clients” behind them. The DOCSIS Option82 is comprised of the following two suboptions:

- Suboption 1, Circuit ID:

```
Type 1 (1 byte)
Len 4 (1 byte)
Value (8 bytes)
<bit 31,30,.....................0)
<xYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY>
```

where the MSB indicates if the attached device is a cable interface.

x=1 Cable Modem REQ

x=0 CPE device (Behind the cable interface with the cable interface MAC address shown in suboption 2.)

The rest of the bits make up the SNMP index to the CMTS interface.

Y=0xYYYYYYY is the SNMP index to the CMTS interface.

- Suboption 2, MAC address of the cable interface:

```
Type 2 (1 byte)
Len 6 (1 byte)
Value xxxx.xxxx.xxxx (6 bytes)
```

Overview of Scripts

This section lists the scripts applicable to cable interface configuration.

Two-way Cable Modem Scripts

To support two-way configurations at a subscriber site, use these scripts:

- **Relay.tcl**
- **SetRouter.tcl**

Telco Return Cable Modem Scripts

To support telco return and two-way cable interface configurations on the same cable interface card or chassis, use these scripts:

- **PostClientLookup.tcl**
- **PrePacketEncode.tcl**

Placement of Scripts

Windows NT

For CNR running on Windows NT, place the appropriate scripts in the following directory:

```
\program files\network registrar\extensions\dhcp\scripts\tcl
```

Solaris

For CNR running on Solaris, place the appropriate scripts in the following directory:

```
/opt/nwreg2/extensions/dhcp/scripts/tcl
```

Activating Scripts in Cisco Network Registrar

To activate the scripts after you have placed them in the appropriate directory:

Step 1 Open up a text editor.

Step 2 Open one of the scripts at the nrcmd> command prompt.

Step 3 Create the extension points and attach them to the system.

Note The easiest way to do this is to simply cut and paste the command lines from the scripts to the nrcmd> command line.

Step 4 After you have created and attached the extension points, do a dhcp reload.
The scripts are active.

Configuring the Cisco CMTS Routers to Use Scripts

Each cable interface must be set up as a BOOTP forwarder and have the relay option enabled. The primary and secondary IP addresses for each cable interface must be in sync with the CNR tool.

To properly communicate with scripts in the system, use the following commands on the Cisco CMTS router:

- To enable option 82, use the **ip dhcp relay info option** command.
- To disable the validation of DHPC relay agent information in forwarded BOOTREPLY messages, use the **no ip dhcp relay information option check** command.

Note You can also use the cable dhcp-giaddr command in cable interface configuration mode to modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets to provide a relay IP address before packets are forwarded to the DHCP server. Use this command to set a “policy” option such that primary addresses are used for CMs and secondary addresses are used for hosts behind the CMs.

Configuring the System Default Policy

Add these options to the system default policy for:

- Cable modems to support on your network
- PCs to support behind each cable interface on your network

Cable Modems

Define these settings following the CNR tool documentation:

- TFTP server (IP address) for those cable interfaces using BOOTP
- Time-server (IP address)
- Time-offset (Hex value, 1440 for Eastern Standard Time)
- Packet-siaddr (IP address of CNR)
- Router (set to 0.0.0.0)
- Boot-file (name of .cm file for those cable interfaces using BOOTP)
- Packet-file-name (.cm file name)

PCs

Define these settings following the CNR tool documentation:

- Domain name
- Name servers (IP address of DNS servers)

Creating Selection Tag Scopes

General

When you create your scope selection tags:

Step 1 Cut and paste the scope selection tag create commands from the scripts into the nrcmd> command line.
Note These names have to be exactly as they appear in the scripts.

Step 2 Then attach the selection tags to the appropriate scripts:
Example:

CM_Scope tagCablemodem

PC_Scope tagComputer

Telco Return for the Cisco uBR7200 Series Router

Before You Begin

Note If you are using the prepacketencode and postclientlookup .tcl scripts for telco return, the telco return scope does not have a selection tag associated to the scope.

SUMMARY STEPS

1. Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.
2. Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

DETAILED STEPS

Step 1 Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.

Step 2 Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

Creating Network Scopes

Following is an example for creating scopes for your network. This example assumes two Cisco uBR7200 series universal broadband routers in two locations, with one cable interface card on one Cisco uBR7200 series configured for telco return.

```
cm-toledo1_2-0 10.2.0.0 255.255.0.0 assignable 10.2.0.10-10.2.254.254 tagCablemodem
tagTelcomodem Default GW=10.2.0.1 (assigned by scripts)
cm-toledo1_3-0 10.3.0.0 255.255.0.0 assignable 10.3.0.10-10.3.254.254 tagCablemodem
tagTelcomodem Default GW=10.3.0.1 (assigned by scripts)
pc-toledo1_2-0 208.16.182.0 255.255.255.248 assignable 208.16.182.2-208.16.182.6 tagComputer
 Default GW=208.16.182.1 (assigned by scripts)
pc-toledo1_3-0 208.16.182.8 255.255.255.248 assignable 208.16.182.10-208.16.182.14 tagComputer
 Default GW=208.16.182.9 (assigned by scripts)
telco_return_2-0 192.168.1.0 255.255.255.0 (No assignable addresses, tag was put on cable
modem primary scope to force telco-return cable modem to pull address from primary scope)
cm-arlington1_2-0 10.4.0.0 255.255.0.0 assignable 10.4.0.10-10.4.254.254 tagCablemodem
Default GW=10.4.0.1 (assigned by scripts)
cm-arlington1_3-0 10.5.0.0 255.255.0.0 assignable 10.5.0.10-10.5.254.254 tagCablemodem
Default GW=10.5.0.1 (assigned by scripts)
pc-arlington1_2-0 208.16.182.16 255.255.255.248 assignable 208.16.182.17-208.16.182.22
tagComputer Default GW=208.16.182.17 (assigned by scripts)
pc-toledo1_3-0 208.16.182.24 255.255.255.248 assignable 208.16.182.2-208.16.182.30 tagComputer
 Default GW=208.16.182.25 (assigned by scripts)
```

Note Remember the last valid address in the .248 subnet range is the broadcast address; do not use this.

Creating Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images

To support Class of Service (CoS), define:

- Scope selection tags—Identifiers that describe types of scope configurations

Note This is needed for Option82.

- Client classes—Class with which a group of clients is associated

Note Scope selection tags are excluded from or included in client-classes.

- Client—Specific DHCP clients and the defined class to which they belong

To assign the CoS or use Option82, make a client entry with a MAC address and point to the appropriate policy. To use client-based MAC provisioning, add a client entry "default - exclude," then put in MAC addresses for all devices (for example, cable interfaces and PCs) in the client tab and select the policy to use, including the appropriate tag.

CNR Steps to Support Subinterfaces

The CNR configuration is done differently if subinterfaces are configured. Here is an example. If you have configured two ISP subinterfaces and one management subinterface on a Cisco uBR7200 series, make sure that the management subinterface is the first subinterface that is configured. If cable interface three—c3/0—is being used, create c3/0.1, c3/0.2 and c3/0.3 as three subinterfaces and c3/0.1 as the first subinterface configured as the management subinterface.

Note The Cisco uBR7200 series requires management subinterfaces to route DHCP packets from CMs when they first initialize because the Cisco uBR7200 series does not know the subinterfaces they belong to until it has seen the IP addresses assigned to them by gleaning DHCP reply message from CNR.

In CNR, complete the following steps for such a configuration:

SUMMARY STEPS

1. Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag
2. Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope
3. Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag
4. Configure two client classes; for example, isp1-client-class and isp2-client-class
5. Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag
6. Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag
7. Enable client class processing from the scope-selection-tag window

DETAILED STEPS

Step 1 Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag

Step 2 Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope

Step 3 Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag

Step 4 Configure two client classes; for example, isp1-client-class and isp2-client-class

Step 5 Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag

Step 6 Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag

Step 7 Enable client class processing from the scope-selection-tag window
Overlapping address ranges cannot be configured on these subinterfaces because software gleans the DHCP reply to figure out the subinterface it really belongs to. Although CNR can be configured with overlapping address range scopes, it cannot be used to allocate addresses from these scopes.

Additional References

The following sections provide references related to Cisco Network Registrar for use with the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cisco Network Registrar documentation	• Go to: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/tsd_products_support_series_home.html
Frequently Asked Questions	• *CNR and DHCP FAQs for Cable Environment* http://www.cisco.com/en/US/tech/tk86/tk808/technologies_q_and_a_item09186a008009434c.shtml
CNR configuration recommendations for performance and troubleshooting tips.	• *Recommended CNR Settings and Management* http://www.cisco.com/warp/public/477/CNR/cnr_best_settings.html

Related Topic	Document Title
Cisco CMTS Commands	• *Cisco IOS CMTS Cable Command Reference Guide* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

Standards	Title
SP-CMCI-I02-980317	Cable Modem to Customer PremiseEquipment Interface Specification http://www.cablemodem.com)
SP-RFI-I04-980724	*Radio Frequency Interface Specification* http://www.cablemodem.com)
SP-CMTRI-I01-970804	*Cable Modem Telephony Return Interface Specification* (http://www.cablemodem.com)

MIBs

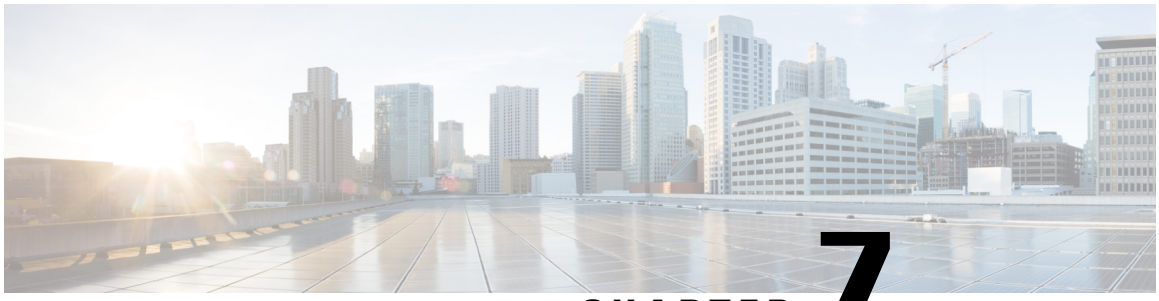
MIBs	MIBs Link
Cisco IOS MIBs Tools	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 7

DHCP, ToD, and TFTP Services for the CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure Cisco Cable Modem Termination System (CMTS) platforms so that they support onboard servers that provide Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and Trivial File Transfer Protocol (TFTP) services for use in Data-over-Cable Service Interface Specifications (DOCSIS) networks. In addition, this document provides information about optional configurations that can be used with external DHCP servers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DHCP, ToD, and TFTP Services

- Cisco recommends the most current Cisco IOS Release 12.1 EC software release for DOCSIS 1.0 operations. For DOCSIS 1.1 operations, Cisco recommends the most current Cisco IOS Release 12.2 BC software release.
- A separate DOCSIS configuration file editor is required to build DOCSIS 1.1 configuration files, because the internal DOCSIS configuration file editor that is onboard the Cisco CMTS router supports only DOCSIS 1.0 configuration files.
- To be able to use the Cisco CMTS as the ToD server, either alone or along with other, external ToD servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

Restrictions for DHCP, ToD, and TFTP Services

- The “all-in-one” configuration should not be used as the only set of servers except for small cable plants (approximately 2,500 cable modems, lab environments, initial testing, small deployments, and troubleshooting. The “all-in-one” configuration can be used in larger networks, however, to supplement other redundant and backup servers.

Note The CMTS does not support the configuration of both Local DHCP Pools and DHCP Relay at the same time.

- The ToD server must use the UDP protocol to conform to DOCSIS specifications.
- For proper operation of the DOCSIS network, especially a DOCSIS 1.1 network using BPI+ encryption and authentication, the system clock on the Cisco CMTS must be set accurately. You can achieve this by manually using the **set clock** command, or by configuring the CMTS to use either the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP).
- The internal DHCP server that is onboard the Cisco CMTS router does not support the **cable source-verify** command.
- Cisco cBR series routers do not support internal DHCP servers.

Information About DHCP, ToD, and TFTP Services

This section provides the following information about the DHCP, ToD, and TFTP Services feature, and its individual components:

Feature Overview

All Cisco CMTS platforms support onboard servers that provide DHCP, ToD, and TFTP proxy-services for use in DOCSIS cable networks. These servers provide the registration services needed by DOCSIS 1.0- and 1.1-compliant cable modems:

- Internal DHCP Servers—Provides the cable modem with an IP address, a subnet mask, default gateway, and other IP related parameters. The cable modem connects with the DHCP server when it initially powers on and logs on to the cable network.
- External DHCP Servers—Provides DHCP services. External DHCP servers are usually part of an integrated provisioning system that is more suitable when managing large cable networks.
- Time-of-DayServer_—Provides an RFC 868 -compliant ToD service so that cable modems can obtain the current date and time during the registration process. The cable modem connects with the ToD server after it has obtained its IP address and other DHCP-provided IP parameters.

Although cable modems do not need to successfully complete the ToD request before coming online, this allows them to add accurate timestamps to their event logs so that these logs are coordinated to the clock used on the CMTS. In addition, having the accurate date and time is essential if the cable modem is trying to register with Baseline Privacy Interface Plus (BPI+) encryption and authentication.

- External TFTP_Server—Downloads the DOCSIS configuration file to the cable modem. The DOCSIS configuration file contains the operational parameters for the cable modem. The cable modem downloads its DOCSIS configuration file after connecting with the ToD server.

You can configure and use each server separately, or you can configure an “all-in-one” configuration so that the CMTS acts as a DHCP, ToD, and TFTP server. With this configuration, you do not need any additional servers, although additional servers provide redundancy, load-balancing, and scalability.

Note You can add additional servers in a number of ways. For example, most cable operators use Cisco Network Registrar (CNR) to provide the DHCP and TFTP servers. ToD servers are freely available for most workstations and PCs. You can install the additional servers on one workstation or PC or on different workstations and PCs.

Internal DHCP Server

At power-up, DOCSIS cable modems send a broadcast message through the cable interface to find a DHCP server that can provide the information needed for IP connectivity across the network. After the cable modem comes online, the CPE devices connected to the cable modem can also make their own DHCP requests. You can configure all Cisco CMTS platforms to act as DHCP servers that provide the IP addressing and other networking information that is needed by DOCSIS cable modems and their CPE devices.

DHCP Field Options

In its DHCP request message, the cable modem identifies itself by its MAC hardware address. In reply, a DOCSIS-compatible DHCP server should provide, at minimum, the following fields when replying to cable modems that are authorized to access the cable network:

- yiaddr—IP address for the cable modem.

- Subnet Mask (option 1)—IP subnet mask for the cable modem.
- siaddr—IP address for the TFTP server that will provide the DOCSIS configuration file.
- file—Filename for the DOCSIS configuration file that the cable modem must download.
- Router Option (option 3)—IP addresses for one or more gateways that will forward the cable modem traffic.
- Time Server Option (option 4)—One or more ToD servers from which the cable modem can obtain its current date and time.
- Time Offset (option 2)—Universal Coordinated Time (UTC) that the cable modem should use in calculating local time.
- giaddr—IP address for a DHCP relay agent, if the DHCP server is on a different network from the cable modem.
- Log Server Option (option 7)—IP address for one or more SYSLOG servers that the cable modem should send error messages and other logging information (optional).
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the cable modem must make another DHCP request.

If you decide to also provide IP addresses to the CPE devices connected to the cable modems, the DHCP server must also provide the following information for CPE devices:

- yiaddr—IP address for the CPE device.
- Subnet Mask (option 1)—IP subnet mask for the CPE device.
- Router Option, option 3—IP addresses for one or more gateways that will forward the CPE traffic.
- Domain Name Server Option (option 6)—IP addresses for the domain name system (DNS) servers that will resolve hostnames to IP addresses for the CPE devices.
- Domain Name (option 15)—Fully-qualified domain name that the CPE devices should add to their hostnames.
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the CPE device must make another DHCP request.

The DHCP server on the Cisco CMTS can also provide a number of options beyond the minimum that are required for network operation. A basic configuration is suitable for small installations as well as lab and experimental networks.

You can also configure the CMTS in a more complex configuration that uses the functionality of DHCP pools. DHCP pools are configured in a hierarchical fashion, according to their network numbers. A DHCP pool with a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool.

DHCP Security Options

Because the DOCSIS specification requires cable modems to obtain their IP addresses from a DHCP server, cable networks are susceptible to certain types of configuration errors and theft-of-service attacks, including:

- Duplicate IP addresses being assigned to two or more cable modems or CPE devices

- Duplicate MAC addresses being reported by two or more cable modems or CPE devices
- Unauthorized use of a DHCP-assigned IP address as a permanent static address
- One user hijacking a valid IP address from another user and using it on a different network device
- Configuring IP addresses with network addresses that are not authorized for a cable segment
- Unauthorized ARP requests on behalf of a cable segment, typically as part of a theft-of-service attack

To help combat these attacks, the Cisco CMTS dynamically maintains a database that links the MAC and IP addresses of known CPE devices with the cable modems that are providing network access for those CPE devices. The CMTS builds this database using information from both internal and external DHCP servers:

- When using the internal DHCP server, the CMTS automatically populates the database from the DHCP requests and replies that are processed by the server.
- When using an external server, the CMTS populates the database by inspecting all broadcast DCHP transactions that are sent over a cable interface between the cable modems and CPE devices on that interface and the DHCP servers.

Note The Cisco CMTS also monitors IP traffic coming from CPE devices to associate their IP and MAC addresses with the cable modem that is providing their Internet connection.

The CMTS can also use the DHCP Relay Agent Information option (DHCP option 82) to send particular information about a cable modem, such as its MAC address and the cable interface to which it is connected to the DHCP server. If the DHCP server cannot match the information with that belonging to a cable modem in its database, the Cisco CMTS identifies that the device is a CPE device. This allows the Cisco CMTS and DHCP server to retain accurate information about which CPE devices are using which cable modems and whether the devices should be allowed network access.

The DHCP Relay Agent Information option can also be used to identify cloned modems or gather geographical information for E911 and other applications. Using the **cable dhcp-insert** command, users configure the Cisco CMTS to insert downstream, upstream, service class, or hostname descriptors into DHCP packets. Multiple types of strings can be configured as long as the maximum relay information option size is not exceeded.

Multiple DHCP Pools

You can also configure any number of DHCP pools for the DHCP server to use in assigning IP addresses. A single pool can be used for a basic configuration, or you can optionally create separate pools for cable modems and CPE devices. You can also use DHCP address pools to provide special services, such as static IP addresses, to customers who are paying for those service.

When creating multiple DHCP pools, you can configure them independently, or you can optionally create a hierarchical structure of pools that are organized according to their network numbers. A DHCP pool that has a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool. In addition to the inherited characteristics, you can further customize each pool with any number of options.

The advantage of DHCP pools is that you can create a number of different DHCP configurations for particular customers or applications, without having to repeat CLI commands for the parameters that the pools have in common. You can also change the configuration of one pool without affecting customers in other pools.

External DHCP Servers

The Cisco CMTS router provides the following optional configurations that can enhance the operation and security of external DHCP servers that you are using on the DOCSIS cable network:

Cable Source Verify Feature

To combat theft-of-service attacks, you can enable the **cable source-verify** command on the cable interfaces on the Cisco CMTS router. This feature uses the router's internal database to verify the validity of the IP packets that the CMTS receives on the cable interfaces, and provides three levels of protection:

- Internal DHCP Server—Provides the cable modem with an IP address, a subnet mask, default gateway, and other IP related parameters. The cable modem connects with the DHCP server when it initially powers on and logs on to the cable network.
- At the most basic level of protection, the Cable Source Verify feature examines every IP upstream packet to prevent duplicate IP addresses from appearing on the cable network. If a conflict occurs, the Cisco CMTS recognizes only packets coming from the device that was assigned the IP address by the DHCP server. The devices with the duplicate addresses are not allowed network address. The CMTS also refuses to recognize traffic from devices with IP addresses that have network addresses that are unauthorized for that particular cable segment.
- Adding the **dhcp** option to the **cable source-verify** command provides a more comprehensive level of protection by preventing users from statically assigning currently-unused IP addresses to their devices. When the Cisco CMTS receives a packet with an unknown IP address on a cable interface, the CMTS drops the packet but also issues a DHCP LEASEQUERY message that queries the DHCP servers for any information about the IP and MAC addresses of that device. If the DHCP servers do not return any information about the device, the CMTS continues to block the network access for that device.
- When you use the **dhcp** option, you can also enable the **leasetimer** option, which instructs the Cisco CMTS to periodically check its internal CPE database for IP addresses whose lease times have expired. The CPE devices that are using expired IP addresses are denied further access to the network until they renew their IP addresses from a valid DHCP server. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices.
- In addition to the dhcp option, you can also configure prefix-based source address verification (SAV) on the Cisco CMTS using the cable source-verify group command. A CM may have a static IPv4 or IPv6 prefix configured, which belongs to an SAV group. When the SAV prefix processing is enabled on the Cisco CMTS, the source IP address of the packets coming from the CM is matched against the configured prefix and SAV group (for that CM) for verification. If the verification fails, the packets are dropped, else the packets are forwarded for further processing. For more information on SAV prefix processing and SAV prefix configuration, see Prefix-based Source Address Verification , on page 140 and Configuring Prefix-based Source Address Verification, on page 159

Prefix-based Source Address Verification

The Source Address Verification (SAV) feature verifies the source IP address of an upstream packet to ensure that the SID/MAC and IP are consistent. The DOCSIS 3.0 Security Specification introduces prefix-based SAV where every CM may have static IPv4 or IPv6 prefixes configured. These prefixes are either preconfigured on the CMTS, or are communicated to the CMTS during CM registration. The Cisco CMTS uses these configured prefixes to verify the source IP address of all the incoming packets from that CM.

An SAV group is a collection of prefixes. A prefix is an IPv4 or IPv6 subnet address. You can use the cable source-verify group command in global configuration mode to configure SAV groups. A total of 255 SAV

groups are supported on a CMTS, with each SAV group having a maximum of four prefixes. Prefixes can be configured using the prefix command.

During registration, CMs communicate their configured static prefixes to the CMTS using two TLVs, 43.7.1 and 43.7.2. The TLV 43.7.1 specifies the SAV prefix group name that the CM belongs to, and TLV 43.7.2 specifies the actual IPv4 or IPv6 prefix. Each CM can have a maximum of four prefixes configured. When the Cisco CMTS receives these TLVs, it first identifies if the specified SAV group and the prefixes are already configured on the Cisco CMTS. If they are configured, the Cisco CMTS associates them to the registering CM. However if they are not configured, the Cisco CMTS automatically creates the specified SAV group and prefixes before associating them to the registering CM.

The SAV group name and the prefixes that are provided by these TLVs are considered valid by the Cisco CMTS. The packets received (from the CM) with the source IP address belonging to the prefix specified by the TLV are considered authorized. For example, if a given CM has been configured with an SAV prefix of 10.10.10.0/24, then any packet received from this CM (or CPE behind the CM) that is sourced with this address in the subnet 10.10.10.0/24 is considered to be authorized.

For more information on how to configure SAV groups and prefixes see Configuring Prefix-based Source Address Verification, on page 159.

Smart Relay Feature

The Cisco CMTS supports a Smart Relay feature (the **ip dhcp smart-relay** command), which automatically switches a cable modem or CPE device to secondary DHCP servers or address pools if the primary server runs out of IP addresses or otherwise fails to respond with an IP address. The relay agent attempts to forward DHCP requests to the primary server three times. After three attempts with no successful response from the primary, the relay agent automatically switches to the secondary server.

When you are using the **cable dhcp-giaddr policy** command to specify that the CPE devices should use the secondary DHCP pools corresponding to the secondary addresses on a cable interface, the smart relay agent automatically rotates through the available secondary in a round robin fashion until an available pool of addresses is found. This ensures that clients are not locked out of the network because a particular pool has been exhausted.

GIADDR Field

When using separate IP address pools for cable modems and CPE devices, you can use the **cable dhcp-giaddr policy** command to specify that cable modems should use an address from the primary pool and that CPE devices should use addresses from the secondary pool. The default is for the CMTS to send all DHCP requests to the primary DHCP server, while the secondary servers are used only if the primary server does not respond. The different DHCP servers are specified using the **cable helper** commands.

Beginning with Cisco IOS Release 12.2(33)SCD5, the GIADDR option simply changes the source IP address of the DHCP request so that the DHCP server can use different subnets to assign the right IP address depending on the types of CPE devices (namely cable modems, media terminal adapters [MTA], portal servers [PS], and set-top boxes [STB]). This enables faster processing of IP addresses; and in case the IP address does not belong to the subnets on the DHCP server, there is minimal usage of CPU resources.

DHCP Relay Agent Sub-option

The Cisco IOS Release 12.2(33)SCF2 introduces support for the DHCP Relay Agent Information sub-option (DHCP Option 82, Suboption 9) enhancement to simplify provisioning of the CPE devices. Using this

sub-option, the cable operators can relay the service class or QoS information of the CPE to the DHCP server to get an appropriate IP address.

To provision a CPE, the DHCP server should be made aware of the service class or QoS information of the CPE. The DHCP server obtains this information using the DHCP DISCOVER message, which includes the service class or QoS information of the CM behind which the CPE resides.

During the provisioning process, the Cisco CMTS uses the DHCPv4 Relay Agent Information sub-option to advertise information about the service class or QoS profile of the CMs to the DHCP server. Using the same technique, the CPE information is relayed to the DHCP server to get an appropriate IP address.

To enable the service classes option, the service class name specified in the CM configuration file must be configured on the Cisco CMTS. This is done by using the **cable dhcp-insert service-class** command.

To configure service-class or QoS-profile on the Cisco CMTS, see Configuring DHCP Service, on page 145.

Note To insert service class relay agent information option into the DHCP DISCOVER messages, the **ip dhcp relay information option-insert** command must be configured on the bundle interface.

Time-of-Day Server

The Cisco CMTS can function as a ToD server that provides the current date and time to the cable modems and other customer premises equipment (CPE) devices connected to its cable interfaces. This allows the cable modems and CPE devices to accurately timestamp their Simple Network Management Protocol (SNMP) messages and error log entries, as well as ensure that all of the system clocks on the cable network are synchronized to the same system time.

Tip The initial ToD server on the Cisco CMTS did not work with some cable modems that used an incompatible packet format. This problem was resolved in Cisco IOS Release 12.1(8)EC1 and later 12.1 EC releases, and in Cisco IOS Release 12.2(4)BC1 and later 12.2 BC releases.

The DOCSIS 1.0 and 1.1 specifications require that all DOCSIS cable modems request the following time-related fields in the DHCP request they send during their initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, in the form of the number of seconds that the device's timestamp is offset from Greenwich Mean Time (GMT).
- Time Server Option (option 4)—Specifies one or more IP addresses for a ToD server.

After a cable modem successfully acquires a DHCP lease time, it then attempts to contact one of the ToD servers provided in the list provided by the DHCP server. If successful, the cable modem updates its system 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 modem eventually times out, logs the failure with the CMTS, and continues on with the initialization process. The cable modem can come online without receiving a reply from a ToD server, but it must periodically continue to reach the ToD server at least once in every five-minute period until it successfully receives a ToD reply. Until it reaches a ToD server, the cable modem must initialize its system clock to midnight on January 1, 1970 GMT.

Note Initial versions of the DOCSIS 1.0 specification specified that the cable device must obtain a valid response from a ToD server before continuing with the initialization process. This requirement was removed in the released DOCSIS 1.0 specification and in the DOCSIS 1.1 specifications. Cable devices running older firmware that is compliant with the initial DOCSIS 1.0 specification, however, might require receiving a reply from a ToD server before being able to come online.

Because cable modems will repeatedly retry connecting with a ToD server until they receive a successful reply, you should consider activating the ToD server on the Cisco CMTS, even if you have one or more other ToD servers at the headend. This ensures that an online cable modem will always be able to connect with the ToD server on the Cisco CMTS, even if the other servers go down or are unreachable because of network congestion, and therefore will not send repeated ToD requests.

Tip To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See Creating and Configuring a DHCP Address Pool for Cable Modems, on page 145 for details on this configuration.

In addition, although the DOCSIS specifications do not require that a cable modem successfully obtain a response from a ToD server before coming online, not obtaining a timestamp could prevent the cable modem from coming online in the following situations:

- If DOCSIS configuration files are being timestamped, to prevent cable modems from caching the files and replaying them, the clocks on the cable modem and CMTS must be synchronized. Otherwise, the cable modem cannot determine whether a DOCSIS configuration file has the proper timestamp.
- If cable modems register using Baseline Privacy Interface Plus (BPI+) authentication and encryption, the clocks on the cable modem and CMTS must be synchronized. This is because BPI+ authorization requires that the CMTS and cable modem verify the timestamps on the digital certificates being used for authentication. If the timestamps on the CMTS and cable modem are not synchronized, the cable modem cannot come online using BPI+ encryption.

Note DOCSIS cable modems must use RFC 868 -compliant ToD server to obtain the current system time. They cannot use the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) service for this purpose. However, the Cisco CMTS can use an NTP or SNTP server to set its own system clock, which can then be used by the ToD server. Otherwise, you must manually set the clock on the CMTS using the **clock set** command each time that the CMTS boots up.

Tip Additional servers can be provided by workstations or PCs installed at the cable headend. UNIX and Solaris systems typically include a ToD server as part of the operating system, which can be enabled by putting the appropriate line in the inetd.conf file. Windows systems can use shareware servers such as Greyware and Tardis. The DOCSIS specifications require that the ToD servers use the User Datagram Protocol (UDP) protocol instead of the TCP protocol for its packets.

TFTP Server

All Cisco CMTS platforms can be configured to provide a TFTP server that can provide the following types of files to DOCSIS cable modems:

- DOCSIS Configuration File—After a DOCSIS cable modem has acquired a DHCP lease and attempted to contact a ToD server, the cable modem uses TFTP to download a DOCSIS configuration file from an authorized TFTP server. The DHCP server is responsible for providing the name of the DOCSIS configuration file and IP address of the TFTP server to the cable modem.
- Software Upgrade File—If the DOCSIS configuration file specifies that the cable modem must be running a specific version of software, and the cable modem is not already running that software, the cable modem must download that software file. For security, the cable operator can use different TFTP servers for downloading DOCSIS configuration files and for downloading new software files.
- Cisco IOS Configuration File—The DOCSIS configuration file for Cisco cable devices can also specify that the cable modem should download a Cisco IOS configuration file that contains command-line interface (CLI) configuration commands. Typically this is done to configure platform-specific features such as voice ports or IPSec encryption.

Note Do not confuse the DOCSIS configuration file with the Cisco IOS configuration file. The DOCSIS configuration file is a binary file in the particular format that is specified by the DOCSIS specifications, and each DOCSIS cable modem must download a valid file before coming online. In contrast, the Cisco IOS configuration file is an ASCII text file that contains one or more Cisco IOS CLI configuration commands. Only Cisco cable devices can download a Cisco IOS file.

All Cisco CMTS platforms can be configured as TFTP servers that can upload these files to the cable modem. The files can reside on any valid device but typically should be copied to the Flash memory device inserted into the Flash disk slot on the Cisco CMTS.

In addition, the Cisco CMTS platform supports an internal DOCSIS configuration file editor in Cisco IOS Release 12.1(2)EC, Cisco IOS Release 12.2(4)BC1, and later releases. When you create a DOCSIS configuration file using the internal configuration file editor, the CMTS stores the configuration file in the form of CLI commands. When a cable modem requests the DOCSIS configuration file, the CMTS then dynamically creates the binary version of the file and uploads it to the cable modem.

Note The internal DOCSIS configuration file editor supports only DOCSIS 1.0 configuration files. To create DOCSIS 1.1 configuration files, you must use a separate configuration editor, such as the Cisco DOCSIS Configurator tool, which at the time of this document's publication is available on Cisco.com at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf

For enhanced security, current versions of Cisco IOS software for Cisco CMTS platforms include a "TFTP Enforce" feature (**cable tftp-enforce** command) that allows you to require that all cable modems must attempt a TFTP download through the cable interface before being allowed to come online. This prevents a common theft-of-service attack in which hackers reconfigure their local network so that a local TFTP server downloads an unauthorized DOCSIS configuration file to the cable modem. This ensures that cable modems download only a DOCSIS configuration file that provides the services they are authorized to use.

Benefits

- The “all-in-one” configuration allows you to set up a basic cable modem network without having to invest in additional servers and software. This configuration can also help troubleshoot plant and cable modem problems.
- The DHCP configuration can more effectively assigns and manages IP addresses from specified address pools within the CMTS to the cable modems and their CPE devices.
- The Cisco CMTS can act as a primary or backup ToD server to ensure that all cable modems are synchronized with the proper date and time before coming online. This also enables cable modems to come online more quickly because they will not have to wait for the ToD timeout period before coming online.
- The ToD server on the Cisco CMTS ensures that all devices connected to the cable network are using the same system clock, making it easier for you to troubleshoot system problems when you analyze the debugging output and error logs generated by many cable modems, CPE devices, the Cisco CMTS, and other services.
- The Cisco CMTS can act as a TFTP server for DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files.
- Aa separate workstation or PC is not required to create and store DOCSIS configuration files.
- The “TFTP Enforce” feature ensures that users download only an authorized DOCSIS configuration file and prevents one of the most common theft-of-service attacks.

How to Configure DHCP, ToD, and TFTP Services

See the following configuration tasks required to configure DHCP service, time-of-day service, and TFTP service on a Cisco CMTS:

All procedures are required unless marked as optional (depending on the desired network configuration and applications).

Configuring DHCP Service

To configure the DHCP server on the Cisco CMTS, use the following procedures to create the required address pools for the server to use. You can create one pool for all DHCP requests (cable modems and CPE devices), or separate pools for cable modems and for CPE devices, as desired.

Creating and Configuring a DHCP Address Pool for Cable Modems

To use the DHCP server on the Cisco CMTS, you must create at least one address pool that defines the IP addresses and other network parameters that are given to cable modems that make DHCP requests. To create an address pool, use the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool local` `Router(dhcp-config)#`	Creates a DHCP address pool and enters DHCP pool configuration file mode. The *name* can be either an arbitrary string, such as **service**, or a number, such as **1**.
Step 4	**network** *network-number* [*mask*] **Example:** `Router(dhcp-config)# network 10.10.10.0 255.255.0.0` `Router(dhcp-config)#`	Configures the address pool with the specified *network-number* and subnet *mask* , which are the DHCP *yiaddr* field and Subnet Mask (DHCP option 1) field. If you do not specify the *mask* value, it s to 255.255.255.255. **Note** To create an address pool with a single IP address, use the **host** command instead of **network**.
Step 5	**bootfile** *filename* **Example:** `Router(dhcp-config)# bootfile platinum.cm` `Router(dhcp-config)#`	Specifies the name of the default DOCSIS configuration file (the DHCP *file* field) for the cable modems that are assigned IP addresses from this pool. The *filename* should be the exact name (including path) that is used to request the file from the TFTP server.
Step 6	**next-server** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# next-server 10.10.11.1` `Router(dhcp-config)#`	Specifies the IP address (the DHCP *siaddr* field) for the next server in the boot process of a DHCP client. For DOCSIS cable modems, this is the IP address for the TFTP server that provides the DOCSIS configuration file. You must specify at least one IP address, and can optionally specify up to eight IP addresses, in order of preference.
Step 7	**default-router** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# default-router 10.10.10.12` `Router(dhcp-config)#`	Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in their order of preference (*address* is the most preferred server, *address2* is the next most preferred, and so on). **Note** The first IP address must be the IP address for the cable interface that is connected to cable modems using this DHCP pool.

	Command or Action	Purpose
Step 8	**option 2 hex** *gmt-offset* **Example:** `Router(dhcp-config)# option 2 hex FFFF.8F80` `Router(dhcp-config)#`	Specifies the Time Offset field (DHCP option 2), which is the local time zone, specified as the number of seconds, in hexadecimal, offset from Greenwich Mean Time (GMT). The following are some sample values for *gmt-offset* : FFFF.8F80 = Offset of –8 hours (–28800 seconds, Pacific Time) FFFF.9D90 = Offset of –7 hours (Mountain Time) FFFF.ABA0 = Offset of –6 hours (Central Time) FFFF.B9B0 = Offset of –5 hours (Eastern Time)
Step 9	**option 4 ip** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# option 4 ip 10.10.10.13 10.10.11.2` `Router(dhcp-config)#`	Specifies the Time Server Option field (DHCP option 4), which is the IP address of the time-of-day (ToD) server from which the cable modem can obtain its current date and time. You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in their order of preference. **Note** If you want to use the Cisco CMTS as the ToD server, you must enter its IP address as part of this command.
Step 10	**option 7 ip** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# option 7 ip 10.10.10.13` `Router(dhcp-config)#`	(Optional) Specifies the Log Server Option field (DHCP option 7), which is the IP address for a System Log (SYSLOG) server that the cable modem should send error messages and other logging information. You can optionally specify up to eight IP addresses, listed in their order of preference.
Step 11	**lease**{*days* [*hours*][*minutes*]|**infinite**} **Example:** `Router(dhcp-config)# lease 0 12 30` `Router(dhcp-config)#`	Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the cable modem. Before the lease expires, the cable modem must make another DHCP request to remain online. The default is one day. You can specify the lease time as follows: • *days* —Duration of the lease in numbers of days (0 to 365). • *hours* — Number of hours in the lease (0 to 23, optional). A *days* value must be supplied before you can configure an *hours* value. • *minutes* — Number of minutes in the lease (0 to 59, optional). A *days* value and an *hours* value must be supplied before you can configure a *minutes* value. • **infinite—** Unlimited lease duration. **Note** In most cable networks, cable modems cannot come online if the lease time is less than 3 minutes. For stability in most cable networks, the minimum lease time should be 5 minutes.
Step 12	**client-identifier** *unique-identifier* **Example:** `Router(dhcp-config)# client-identifier 0100.0C01.0203.04` `Router(dhcp-config)#`	(Optional) Specifies the MAC address that identifies the particular cable modem that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier (“01”) with the six-byte MAC address for the cable modem. For example, to specify a cable modem with the MAC address of 9988.7766.5544, specify a *unique-identifier* of 0199.8877.6655.44.

	Command or Action	Purpose
		Note This option should be used only for DHCP pools that assign a static address to a single cable modem.
Step 13	**cable dhcp-insert** {**downstream-description** | **hostname** | **service-class** | **upstream-description**} **Example:** `Router(dhcp-config)# cable dhcp-insert service-class` `Router(dhcp-config)#`	(Optional) Specifies which descriptors to append to DHCP packets. The DHCP server can then use these descriptors to identify cable modem clones and extract geographical information: • **downstream-description—** Appends received DHCP packets with downstream port descriptors. • **hostname—** Appends received DHCP packets with router host names. • **service-class—** Appends received DHCP packets with router service class. • **upstream-description—** Appends received DHCP packets with upstream port descriptors. **Note** Multiple types of descriptor strings can be configured as long as the maximum relay information option size is not exceeded.
Step 14	**exit** **Example:** `Router(dhcp-config)# exit` `Router(config)#`	Exits DHCP configuration mode.
Step 15	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Creating and Configuring a DHCP Address Pool for CPE Devices

In addition to providing IP addresses for cable modems, the DHCP server on the Cisco CMTS server can optionally provide IP addresses and other network parameters to the customer premises equipment (CPE) devices that are connected to the cable modems on the network. To do so, create a DHCP address pool for those CPE devices, using the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.

Note You can use the same address pools for cable modems and CPE devices, but it simplifies network management to maintain separate pools.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool local`	Creates a DHCP address pool and enters DHCP pool configuration file mode. The *name* can be either an arbitrary string, such as **service**, or a number, such as **1**.
Step 4	**network** *network-number* [*mask*] **Example:** `Router(dhcp-config)# network 10.10.10.0 255.255.0.0`	Configures the address pool with the specified *network-number* and subnet *mask* , which are the DHCP *yiaddr* field and Subnet Mask (DHCP option 1) field. If you do not specify the *mask* value, it defaults to 255.255.255.255. **Note** To create an address pool with a single IP address, use the **host** command instead of **network**.
Step 5	**default-router** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# default-router 10.10.10.12`	Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems and CPE devices in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in order of preference (*address* is the most preferred server, *address2* is the next most preferred, and so on).
Step 6	**dns-server** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# dns-server 10.10.10.13`	Specifies one or more IP address for the Domain Name Server Option (DHCP option 6) field, which are the domain name system (DNS) servers that will resolve host names to IP addresses for the CPE devices. You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in order of preference.
Step 7	**domain-name***domain* **Example:** `Router(dhcp-config)# domain-name cisco.com`	Specifies the Domain Name (DHCP option 15) field, which is the fully-qualified domain name that the CPE devices should add to their hostnames. The *domain* parameter should be the domain name used by devices on the cable network.

	Command or Action	Purpose
Step 8	**lease** {*days* [*hours*][*minutes*]|**infinite**} **Example:** `Router(dhcp-config)# lease 0 12 30`	Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the CPE device. Before the lease expires, the CPE device must make another DHCP request to remain online. The default is one day. You can specify the lease time as follows: • *days* —Duration of the lease in numbers of days (0 to 365). • *hours* — Number of hours in the lease (0 to 23, optional). A *days* value must be supplied before you can configure an *hours* value. • *minutes* — Number of minutes in the lease (0 to 59, optional). A *days* value and an *hours* value must be supplied before you can configure a *minutes* value. • **infinite —** Unlimited lease duration.
Step 9	**client-identifier** *unique-identifier* **Example:** `Router(dhcp-config)# client-identifier 0100.0C01.0203.04`	(Optional) Specifies the MAC address that identifies a particular CPE device that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier ("01") with the six-byte MAC address for the device. For example, so specify a device with the MAC address of 9988.7766.5544, specify a unique-identifier of 0199.8877.6655.44. **Note** This option should be used only for DHCP pools that assign a static address to a single CPE device.
Step 10	**cable dhcp-insert** {**downstream-description** | **hostname** | **service-class** | **upstream-description**} **Example:** `Router(dhcp-config)# cable dhcp-insert service-class`	(Optional) Specifies which descriptors to append to DHCP packets. The DHCP server can then use these descriptors to identify CPEs and extract geographical information: • **downstream-description—** Appends received DHCP packets with downstream port descriptors. • **hostname—** Appends received DHCP packets with router host names. • **service-class—** Appends received DHCP packets with router service class. • **upstream-description—** Appends received DHCP packets with upstream port descriptors.
Step 11	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Time-of-Day Service

This section provides procedures for enabling and disabling the time-of-day (ToD) server on the Cisco CMTS routers.

Prerequisites

To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See Creating and Configuring a DHCP Address Pool for Cable Modems for details on this configuration when using the internal DHCP server.

Enabling Time-of-Day Service

To enable the ToD server on a Cisco CMTS, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**service udp-small-servers max-servers no-limit** **Example:** `Router(config)# service udp-small-servers max-servers no-limit` `Router(config)#`	Enables use of minor servers that use the UDP protocol (such as ToD, echo, chargen, and discard). The max-servers no-limit option allows a large number of cable modems to obtain the ToD server at one time, in the event that a cable or power failure forces many cable modems offline. When the problem has been resolved, the cable modems can quickly reconnect.
Step 4	**cable time-server** **Example:** `Router(config)# cable time-server` `Router(config)#`	Enables the ToD server on the Cisco CMTS.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Disabling Time-of-Day Service

To disable the ToD server, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` ` Router(config)#`	Enters global configuration mode.
Step 3	**no cable time-server** **Example:** `Router(config)# cable time-server` `Router(config)#`	Disables the ToD server on the Cisco CMTS.
Step 4	**no service udp-small-servers** **Example:** `Router(config)# no service udp-small-servers` `Router(config)#`	(Optional) Disables the use of all minor UDP servers. **Note** Do not disable the minor UDP servers if you are also enabling the other DHCP or TFTP servers.
Step 5	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Configuring TFTP Service

To configure TFTP service on a Cisco CMTS where the CMTS can act as a TFTP server and download a DOCSIS configuration file to cable modems, perform the following steps:

- Create the DOCSIS configuration files using the DOCSIS configuration editor of your choice.
- You can also use the internal DOCSIS configuration file editor on the Cisco CMTS to create DOCSIS configuration files.
- Copy all desired files (DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files) to the Flash memory device on the Cisco CMTS. Typically, this is done by placing the files first on an external TFTP server, and then using TFTP commands to transfer them to the router's Flash memory.

Note If you are using the internal DOCSIS configuration editor on the Cisco CMTS to create the DOCSIS configuration files, you do not need to copy the files to a Flash memory device because they are already part of the router's configuration.

- Enable the TFTP server on the Cisco CMTS with the **tftp-server** command.
- Optionally enable the TFTP enforce feature so that cable modems must attempt a TFTP download of the DOCSIS configuration file through the cable interface with the CMTS before being allowed to come online.

Each configuration task is required unless otherwise listed as optional.

Step 1 Use the **show file systems** command to display the Flash memory cards that are available on your CMTS, along with the free space on each card and the appropriate device names to use to access each card.
Most configurations of the Cisco CMTS platforms support both linear Flash and Flash disk memory cards. Linear Flash memory is accessed using the **slot0** (or **flash**) and **slot1** device names. Flash disk memory is accessed using the **disk0** and **disk1** device names.

For example, the following command shows a Cisco uBR7200 series router that has two linear Flash memory cards installed. The cards can be accessed by the **slot0** (or **flash**) and **slot1** device names.

Example:

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
    48755200    48747008     flash     rw   slot0: flash:
    16384000    14284000     flash     rw   slot1:
    32768000    31232884     flash     rw   bootflash:
*          -           -      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      507263     nvram     rw   nvram:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
```

```
           -           -   network     rw   scp:
Router#
```

The following example shows a Cisco uBR10012 router that has two Flash disk cards installed. These cards can be accessed by the **disk0** and **sec-disk0** device names.

Example:

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -     flash     rw   slot0: flash:
           -           -     flash     rw   slot1:
    32768000    29630876     flash     rw   bootflash:
*  128094208    95346688      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -     flash     rw   sec-slot0:
           -           -     flash     rw   sec-slot1:
*  128094208    95346688      disk     rw   sec-disk0:
           -           -      disk     rw   sec-disk1:
    32768000    29630876     flash     rw   sec-bootflash:
           -           -     nvram     rw   sec-nvram:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      505523      nvram     rw   nvram:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
Router#
```

Tip The Cisco uBR10012 router supports redundant processors, a primary and a secondary, and each processor contains its own Flash memory devices. You typically do not have to copy files to the secondary Flash memory devices (which have the **sec** prefix) because the Cisco uBR10012 router synchronizes the secondary processor to the primary one.

Step 2 Verify that the desired Flash memory card has sufficient free space for all of the files that you want to copy to the CMTS.

Step 3 Use the **ping** command to verify that the remote TFTP server that contains the desired files is reachable. For example, the following shows a **ping** command being given to an external TFTP server with the IP address of 10.10.10.1:

Example:

```
Router# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/6 ms
```

Step 4 Use the **copy tftp** *devname* command to copy each file from the external TFTP server to the appropriate Flash memory card on the CMTS, where *devname* is the device name for the destination Flash memory card. You will then be prompted for the IP address for the external TFTP server and the filename for the file to be transferred.
The following example shows the file docsis.cm being transferred from the external TFTP server at IP address 10.10.10.1 to the first Flash memory disk (disk0):

Example:

```
Router# copy tftp disk0
Address or name of remote host []? 10.10.10.1

Source filename []? config-files/docsis.cm

Destination filename [docsis.cm]?
```

```
Accessing tftp://10.10.10.1/config-file/docsis.cm......
Loading docsis.cm from 10.10.10.1 (via Ethernet2/0): !!!
[OK - 276/4096 bytes]
276 bytes copied in 0.152 secs
Router#
```

Step 5 Repeat Step 4, on page 154 as needed to copy all of the files from the external TFTP server to the Flash memory card on the Cisco CMTS.

Step 6 Use the **dir** command to verify that the Flash memory card contains all of the transferred files.

Example:

```
Router# dir disk0:

Directory of disk0:/
    1  -rw-    10705784   May 30 2002 19:12:46  ubr10k-p6-mz.122-2.8.BC
    2  -rw-        4772   Jun 20 2002 18:12:56  running.cfg.save
    3  -rw-         241   Jul 31 2002 18:25:46  gold.cm
    4  -rw-         225   Jul 31 2002 18:25:46  silver.cm
    5  -rw-         231   Jul 31 2002 18:25:46  bronze.cm
    6  -rw-          74   Oct 11 2002 21:41:14  disable.cm
    7  -rw-     2934028   May 30 2002 11:22:12  ubr924-k8y5-mz.bin
    8  -rw-     3255196   Jun 28 2002 13:53:14  ubr925-k9v9y5-mz.bin
128094208 bytes total (114346688 bytes free)
Router#
```

Step 7 Use the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal

Router(config)#
```

Step 8 Use the **tftp-server** command to specify which particular files can be transferred by the TFTP server that is onboard the Cisco CMTS. You can also use the **alias** option to specify a different filename that the DHCP server can use to refer to the file. For example, the following commands enable the TFTP transfer of the configuration files and software upgrade files:

Example:

```
Router(config)# tftp-server disk0:gold.cm alias gold.cm

Router(config)# tftp-server disk0:silver.cm alias silver.cm

Router(config)# tftp-server disk0:bronze.cm alias bronze.cm

Router(config)# tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile

Router(config)# tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile

Router(config)#
```

Note The **tftp-server** command also supports the option of specifying an access list that restricts access to the particular file to the IP addresses that match the access list.

Step 9 (Optional) Use the following command to enable the use of the UDP small servers, and to allow an unlimited number of connections at one time. This will allow a large number of cable modems that have gone offline due to cable or power failure to rapidly come back online.

Example:

```
Router(config)# service udp-small-servers max-servers no-limit
```

```
Router(config)#
```

Step 10 (Optional) Use the **cable tftp-enforce** command in interface configuration mode to require that each cable modem perform a TFTP download of its DOCSIS configuration file through its cable interface with the CMTS before being allowed to come online. This can prevent the most common types of theft-of-service attacks in which users configure their local networks so as to download an unauthorized configuration file to their cable modems.

Example:

```
Router(config)# interface cable
x/y

Router(config-if)# cable tftp-enforce

Router(config-if)#
```

You can also specify the **mark-only** option so that cable modems can come online without attempting a TFTP download, but the cable modems are marked in the **show cable modems** command so that network administrators can investigate the situation further before taking any action.

Example:

```
Router(config)# interface cable
x/y

Router(config-if)# cable tftp-enforce mark-only

Router(config-if)#
```

Configuring A Basic All-in-One Configuration

The basic all-in-one configuration requires configuring the DHCP, ToD, and TFTP servers, as described in the following sections in this document:

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the Configuring TFTP Service, on page 153.
- Dynamically create the DOCSIS configuration files with the **cable config-file** command.

For an example of a basic all-in-one configuration, see the Basic All-in-One Configuration Example, on page 166.

Configuring an Advanced All-in-One Configuration

The advanced all-in-one configuration sample is identical to the basic configuration except that it uses a hierarchy of DHCP pools. Any DHCP pool with a network number that is a subset of another pool's network number inherits all the characteristics of that other pool. This saves having to repeat identical commands in the multiple DHCP pool configurations.

For information on the required tasks, see the following sections in this guide:

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the Configuring TFTP Service, on page 153.
- Dynamically create the DOCSIS configuration files with the **cable config-file** command.

For an example of an advanced all-in-one configuration, see the Advanced All-in-One Configuration Example, on page 169.

Optimizing the Use of an External DHCP Server

The Cisco CMTS offers a number of options that can optimize the operation of external DHCP servers on a DOCSIS cable network. See the following sections for details. All procedures are optional, depending on the needs of your network and application servers.

Configuring Cable Source Verify Option

To enhance security when using external DHCP servers, you can optionally configure the Cable Source Verify feature with the following procedure.

Restriction

- The Cable Source Verify feature supports only external DHCP servers. It cannot be used with the internal DHCP server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0` `Router(config-if)#`	Enters cable interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	**cable source-verify** [**dhcp** | **leasetimer** *value*] **Example:** `Router(config-if)# cable source-verify dhcp` **Example:** `Router(config-if)# cable source-verify leasetimer 30` `Router(config-if)#`	(Optional) Ensures that the CMTS allows network access only to those IP addresses that DCHP servers issued to devices on this cable interface. The CMTS examines DHCP packets that pass through the cable interfaces to build a database of which IP addresses are valid on which interface. • **dhcp** = (Optional) Drops traffic from all devices with unknown IP addresses, but the CMTS also sends a query to the DHCP servers for any information about the device. If a DHCP server informs the CMTS that the device has a valid IP address, the CMTS then allows the device on the network. • **leasetimer** *value* = (Optional) Specifies how often, in minutes, the router should check its internal CPE database for IP addresses whose lease times have expired. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices. The valid range for value is 1 to 240 minutes, with no default. **Note** The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface.
Step 5	**no cable arp** **Example:** `Router(config-if)# no cable arp` `Router(config-if)#`	(Optional) Blocks Address Resolution Protocol (ARP) requests originating from devices on the cable network. Use this command, together with the **cable source-verify dhcp** command, to block certain types of theft-of-service attacks that attempt to hijack or spoof IP addresses. **Note** Repeat Step 3, on page 157 through Step 5, on page 158 for each desired cable interface.
Step 6	**exit** **Example:** `Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode.
Step 7	**ip dhcp relay information option** **Example:** `Router(config)# ip dhcp relay information option` `Router(config)#`	(Optional) Enables the CMTS to insert DHCP relay information (DHCP option 82) in relayed DHCP packets. This allows the DHCP server to store accurate information about which CPE devices are using which cable modems. You should use this command if you are also using the **cable source-verify dhcp** command.
Step 8	**exit** **Example:**	Exits global configuration mode.

	Command or Action	Purpose
	Note Cisco IOS releases before Release 12.1(2)EC1 used the **cable relay-agent-option** command for this purpose, but current releases should use the **ip dhcp relay information option** command. `Router(config)# exit` `Router#`	

Configuring Prefix-based Source Address Verification

To enhance security when using external DHCP servers, you can configure a prefix-based SAV with the following procedure, beginning in global configuration (config) mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	cable source-verify enable-sav-static **Example:** `Router# cable source-verify enable-sav-static` `Router(config)#`	Enables SAV prefix processing on the Cisco CMTS.
Step 4	**cable source-verify group** *groupname* **Example:** `Router(config)# cable source-verify group sav-1`	Configures the SAV group name. *groupname*— Name of the SAV group with a maximum length of 16 characters.
Step 5	**prefix** [**ipv4_prefix/ipv4_prefix_length** | **ipv6_prefix/ipv6_prefix_length**]	Configures the IPv4 or IPv6 prefix associated with the SAV group. • *ipv4_prefix*— IPv4 prefix associated with the SAV group, specified in the X.X.X.X/X format.

	Command or Action	Purpose
	Example: `Router(config-sav)# prefix 10.10.10.0/24` `Router(config-sav)#`	• ipv4_prefix_length—Length of the IPv4 prefix. The valid range is from 0 to 32. • ipv6_prefix—IPv6 prefix associated with a particular SAV group, specified in the X:X:X:X::/X format. • ipv6_prefix_length—Length of the IPv6 prefix. The valid range is from 0 to 128. A maximum of four prefixes can be configured in a single SAV group. These prefixes can be either IPv4s, IPv6s, or a combination of both.
Step 6	**exit** **Example:** `Router(config-sav)# exit`	Exits SAV configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Optional DHCP Parameters

When using an external DHCP server, the Cisco CMTS supports a number of options that can enhance operation of the cable network in certain applications. To configure these options, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip dhcp smart-relay** **Example:** `Router(config)# ip dhcp smart-relay` `Router(config)#`	(Optional) Enables the DHCP relay agent on the CMTS to automatically switch a cable modem or CPE device to a secondary DHCP server or address pool if the primary DHCP server does not respond to three successive requests. If multiple secondary servers have been defined, the relay agent forwards DHCP requests to the secondary servers in a round robin fashion.
Step 4	**ip dhcp ping packet 0** **Example:** `Router(config)# ip dhcp ping packet 0` `Router(config)#`	(Optional) Instructs the DHCP server to assign an IP address from its pool without first sending an ICMP ping to test whether a client is already currently using that IP address. Disabling the ping option can speed up address assignment when a large number of modems are trying to connect at the same time. However, disabling the ping option can also result in duplicate IP addresses being assigned if users assign unauthorized static IP addresses to their CPE devices. **Note** By default, the DHCP server pings a pool address twice before assigning a particular address to a requesting client. If the ping is unanswered, the DHCP server assumes that the address is not in use and assigns the address to the requesting client.
Step 5	**ip dhcp relay information check** **Example:** `Router(config)# ip dhcp relay information check` `Router(config)#`	(Optional) Configures the DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages. Invalid messages are dropped. **Note** The **ip dhcp relay information** command contains several other options that might be useful for special handling of DHCP packets. See its command reference page in the Cisco IOS documentation for details.
Step 6	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0` `Router(config-if)#`	Enters cable interface configuration mode for the specified cable interface.
Step 7	**cable dhcp-giaddr policy** [**host** | **stb** | **mta** | **ps**] *giaddr* **Example:** `Router(config-if)# cable dhcp-giaddr policy mta 172.1.1.10` `Router(config-if)#`	Sets the DHCP GIADDR field for DHCP request packets to the primary address for cable modems, and the secondary address for CPE devices. This enables the use of separate address pools for different clients. • **host—**Specifies the GIADDR for hosts. • **mta—**Specifies the GIADDR for MTAs. • **ps—**Specifies the GIADDR for PSs. • **stb—**Specifies the GIADDR for STBs. • *giaddr***—**IP addresses of the secondary interface of the bundle interface. **Note** The **cable dhcp-giaddr** command also supports the **primary** option. The **primary** option forces all device types to use only the primary interface IP address as GIADDR and not rotate through the secondary address if the primary address fails.
Step 8	**cable helper-address** *address* [**cable-modem** | **host** | **mta** | **stb**]	(Optional) Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or

	Command or Action	Purpose
	Example: `Router(config-if)# cable helper-address 10.10.10.13` `Router(config-if)#`	subinterface. You can also specify separate servers for cable modems and CPE devices. • *address* = IP address of a DHCP server to which UDP broadcast packets will be sent via unicast packets. • **cable-modem** = Specifies this server should only accept cable modem packets (optional). • **host** = Specifies this server should only accept CPE device packets (optional). • **mta**= Specifies this server should only accept MTA packets (optional). You must also complete Step 9, on page 162. • **stb** = Specifies this server should only accept STB packets (optional). You must also complete Step 9, on page 162. **Note** If you do not specify an option, the helper-address will support all cable devices, and the associated DHCP server will accept DHCP packets from all cable device classes. **Note** If you specify only one option, the other types of devices (cable modem, host, mta, or stb) will not be able to connect with a DHCP server. You must specify each desired option in a separate command **Tip** Repeat this command to specify more than one helper address on each cable interface. You can specify more than 16 helper addresses, but the Cisco IOS software uses only the first 16 valid addresses. **Tip** If you configure different helper addresses on different sub-bundles within a bundle, the cable modem may not come online. We recommend that you use the same helper address on all sub-bundles within a bundle. **Note** The **ip helper-address** command performs a similar function to **cable helper-address**, but it should be used on non-cable interfaces. The **cable helper-address** command should be used on cable interfaces because it is optimized for the operation of DHCP requests on DOCSIS networks.
Step 9	**cable dhcp-parse option**-*optnum* **Example:** `Router(config-if)# cable dhcp-parse option-43` `Router(config-if)#`	(Optional) Enables the parsing of certain DHCP options. • *optnum* = Specifies which option should be enabled. Valid values are **43** or **60**. **Note** If you specified the **mta** or **stb** option in Step 8, on page 161, you must parse DHCP packets to allow for the extraction of cable device classes. **Tip** If you know in advance that certain options are not used by your CMTS, you can disable their parsing using the **no cable dhcp-parse option-optnum** command. **Note** Repeat Step 6, on page 161 through Step 8, on page 161 for each desired cable interface.
Step 10	**cable dhcp-giaddr policy** **Example:** `Router(config-if)# cable dhcp-giaddr policy`	Selects the control policy, so the primary address is used for cable modems and the secondary addresses are used for hosts and other customer premises equipment (CPE) devices. This setting is typically used when the CMs on the interface are configured for routing mode, so that the cabel modems and hosts can use IP addresses on different subnets.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode.
Step 12	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Configuration Examples

This section provides examples for the following configurations:

DHCP Server Examples

The following sections gave sample configurations for configuring DHCP pools for cable modems and CPE devices:

DHCP Pools for Cable Modems

The following examples show three typical DHCP pools for cable modems. Each pool includes the following fields:

- The dhcp pool command defines a unique string for the pool's name, which in this case identifies the DOCSIS configuration file that is to be downloaded to the cable modem.
- The **network** command defines the range of IP addresses for each pool.
- The **bootfile** command specifies the DOCSIS configuration file to be downloaded to the cable modem. In these examples, three DOCSIS configuration files are specified (platinum.cm, gold.cm, and silver.cm).
- The **next-server** command specifies the IP address for the TFTP server.
- The **default-router** command specifies the default gateway.
- The three **option** commands specify the time offset, ToD server, and log server.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The cable modem will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!
ip dhcp pool cm-platinum
   network 10.128.4.0 255.255.255.0
   bootfile platinum.cm
```

```
   next-server 10.128.4.1
   default-router 10.128.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
!
ip dhcp pool cm-gold
   network 10.129.4.0 255.255.255.0
   bootfile gold.cm
   next-server 10.129.4.1
   default-router 10.129.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
!
ip dhcp pool cm-silver
   network 10.130.4.0 255.255.255.0
   bootfile silver.cm
   next-server 10.130.4.1
   default-router 10.130.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
```

DHCP Pools for Disabling Cable Modems

The following examples shows typical DHCP pool configurations for cable modems that disable network access for their attached CPE devices. With this configuration, the cable modem can come online and is able to communicate with the CMTS, but the CPE devices cannot access the cable network. Each pool includes the following fields:

- The DHCP pool name is a unique string that indicates the MAC address for each cable modem that should be disabled.
- The **host** option specifies a single static IP address.
- The **client-identifier** option identifies a particular cable modem to be denied access. The cable modem is identified by the combination of the Ethernet media code (“01”) plus the cable modem’s MAC address.
- The **bootfile** option specifies a DOCSIS configuration file (“disable.cm”) that disables network access.

```
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
    host 10.128.1.9 255.255.255.0
    client-identifier  0100.10aa.aa00.01
    bootfile disable.cm
!
ip dhcp pool DisabledModem(0020.bbbb.0002)
    host 10.128.1.10 255.255.255.0
    client-identifier  0100.20bb.bb00.02
    bootfile disable.cm
ip dhcp pool DisabledModem(1010.9581.7f66)
   host 10.128.1.11 255.255.255.0
   client-identifier 0100.1095.817f.66
   bootfile disable.cm
```

DHCP Pools for CPE Devices

The following examples show a typical DHCP pool for CPE devices. Each pool includes the following fields:

- The **network** command defines the range of IP addresses to be assigned to the CPE devices. Typically, this command specifies a subnet in the secondary address range for the cable interface.
- The **default-router** command specifies the default gateway.
- The **dns-server** command specifies one or more IP addresses for the DNS name-resolution servers that the CPE devices should use.
- The **domain-name** command specifies the fully-qualified domain name that the CPE devices should use.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The CPE device will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 7 0 10
!
```

The following example shows a DHCP pool that assigns a permanent, static IP address to a particular CPE device. This example is identical to the previous pool except for the following commands:

- The **host** command is used (instead of the **network** command) to specify a single static IP address that will be assigned to the CPE device.
- The **client-identifier** command identifies the particular CPE device. The CPE device is identified by the combination of the Ethernet media code (“01”) plus the device’s MAC address (0001.dddd.0001).

```
!
ip dhcp pool staticPC(0001.dddd.0001)
    host 10.254.1.12 255.255.255.0
    client-identifier 0100.01dd.dd00.01
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 7 0 10
```

ToD Server Example

The following example shows a typical ToD server configuration:

```
service udp-small-servers max-servers no-limit
cable time-server
```

These are the only commands required to enable the ToD server.

TFTP Server Example

The following lines are an excerpt from a configuration that includes a TFTP server. Change the files listed with the **tftp-server** command to match the specific files that are on your system.

```
! Enable the user of unlimited small servers
 service udp-small-servers max-servers no-limit
!
...
```

```
! Enable the TFTP server and specify the files that can be
!   downloaded along with their aliases
 tftp-server disk0:gold.cm alias gold.cm
 tftp-server disk0:silver.cm alias silver.cm
 tftp-server disk0:bronze.cm alias bronze.cm
 tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile
 tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile
```

Basic All-in-One Configuration Example

The basic "all-in-one configuration" sample below summarizes all the components described in examples in the Configuration Examples, on page 163. Five DOCSIS configuration files are available. The internal DOCSIS configuration file editor has been used to create four (platinum.cm, gold.cm, silver.cm, and disable.cm), and the fifth file, bronze.cm, has been loaded on to the slot0 Flash memory device. The disable.cm file disables network access for all CPE devices attached to a cable modem, and the other four files provide different levels of Quality-of-Service (QoS).

The configuration has two DHCP pools with two different address spaces. One pool provides IP addresses and platinum-level service for cable modems, and the other pool provides IP addresses for CPE devices.

```
!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime
! turn service password-encryption on to encrypt passwords
no service password-encryption
! provides additional space for longer configuration file
service compress-config
! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
! permits cable modems to obtain Time of Day (TOD) from uBR7100
cable time-server
!
! High performance DOCSIS config file, additional options may be added
!   10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
!   connecting after 150% of guaranteed-bandwidth has been allocated to
!   registered modems. This can be used for peek load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
!   too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
!   additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
! Medium performance DOCSIS config file, additional options may be added
!   5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
```

```
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp
!
! Low performance DOCSIS config file, additional options may be added
!   1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
!   1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix
! Disables the finger server
no ip finger
! Prevents CMTS from looking up domain names / attempting to connect to
!   machines when mistyping commands
no ip domain-lookup
! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1
!
! DHCP reply settings for DOCSIS cable modems.
!   All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of  server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10
!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
!   line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
!   reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
```

```
    lease 1 0 10
!
!
!
interface FastEthernet0/0
  ip address 10.17.123.1 255.255.255.0
  no ip mroute-cache
  no shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems
! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy:  use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
```

```
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West
  cable upstream 3 frequency 37008000
  cable upstream 3 power-level 0
  cable upstream 3 admission-control 150
  no cable upstream 3 shutdown
  no cable arp
  cable source-verify dhcp
  cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
!   this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  speed 19200
line vty 0 4
  session-timeout 60
  login
!
ntp clock-period 17179977
ntp server 192.168.35.51
end
```

Advanced All-in-One Configuration Example

The advanced all-in-one configuration is identical to the basic configuration, except that it uses a hierarchical structure of DHCP pools to provide unique DHCP options, such as static IP addresses, to individual cable modems and CPE devices. The DHCP pools are given unique and relevant names to simplify administration, and the cable modems and CPE devices that use these pools are specified by the **client-identifier** commands.

The DHCP pools for the individual cable modems and CPE devices inherit the options from the parent pools, so you do not need to specify all of the required options for those particular pools. Instead, the new pools need to specify only those commands, such as **client-identifier**, that should be different from the parent pools.

Because the static IP addresses that are given to the cable modems and CPE devices are in the range of 10.1.4.60 and 10.1.4.70, the **ip dhcp exclude** command is used to instruct the DHCP server that it should not hand out addresses in this range to other cable modems or CPE devices.

```
!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime
! turn service password-encryption on to encrypt passwords
no service password-encryption
```

```
! provides additional space for longer configuration file
service compress-config
! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
! permits cable modems to obtain Time of Day (TOD) from uBR7100
cable time-server
!
! High performance DOCSIS config file, additional options may be added
!   10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
!   connecting after 150% of guaranteed-bandwidth has been allocated to
!   registered modems. This can be used for peek load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
!   too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
!   additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
! Medium performance DOCSIS config file, additional options may be added
!   5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp
!
! Low performance DOCSIS config file, additional options may be added
!   1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
!   1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix
! Disables the finger server
no ip finger
! Prevents CMTS from looking up domain names / attempting to connect to
!   machines when mistyping commands
```

```
no ip domain-lookup
! Prevents the issuance of IP addresses in this range, allows for use in
!   static configurations.
ip dhcp excluded-address 10.128.1.60 10.128.1.70
! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1
!
! DHCP reply settings for DOCSIS cable modems.
!   All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of  server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10
!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
!   line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
!   reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 1 0 10
!
! DHCP reply settings for a static IP address for a PC and cable modems
! All settings here will override "default response settings" for this DHCP pool.
! client-identifier is the ethernet MAC address of the device, preceded by 01
!   Thus, the Host with an mac address of 08.00.09.af.34.e2 will ALWAYS get the
!   same IP address
! Lease length, in days, hours, minutes, set to infinite.
! Use a relevant name here, as there will be lots of these entries.
!
ip dhcp pool staticPC(0800.09af.34e2)
    host 10.254.1.12 255.255.255.0
    client-identifier 0108.0009.af34.e2
    client-name staticPC(0800.09af.34e2)
    lease infinite
ip dhcp pool cm-0050.04f9.efa0cm-
   host 10.128.1.65 255.255.255.0
   client-identifier 0100.107b.ed9b.45
   bootfile disable.cm
!
ip dhcp pool cm-0030.d002.41f5
   host 10.128.1.66 255.255.255.0
   client-identifier 0100.107b.ed9b.23
   bootfile silver.cm
!
! DHCP reply settings for a cable modem, to change from default provisioning
! All settings here will override "default response settings" for this DHCP pool.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
!   Thus, the modem with a mac address of 00.10.95.81.7f.66 will ALWAYS get the
!   same IP address
! This cable modem will get the gold.cm config file, and a consistent IP address
```

```
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
!  address with “clear ip dhcp binding <ip-address>” and then reset the modem using
!  "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool goldmodem
    host 10.128.1.67 255.255.255.0
    client-identifier 0100.1095.817f.66
    bootfile gold.cm
!
! DHCP reply settings for a disabled cable modem.
! This will prevent this cable modem user from accessing the network.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
! This cable modem will get the disable.cm config file, and a consistent IP address
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
!  address with “clear ip dhcp binding <ip-address>” and then reset the modem using
!  "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
    host 10.128.1.68 255.255.255.0
    client-identifier 0100.1095.817f.66
    bootfile disable.cm
!
ip dhcp pool DisabledModem(0000.bbbb.0000)
    client-identifier 0100.00bb.bb00.00
    host 10.128.1.69 255.255.255.0
    bootfile disable.cm
!
!
!
interface FastEthernet0/0
  ip address 10.17.123.1 255.255.255.0
  no ip mroute-cache
  no shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems
! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
```

```
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy:  use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West
  cable upstream 3 frequency 37008000
  cable upstream 3 power-level 0
  cable upstream 3 admission-control 150
  no cable upstream 3 shutdown
  no cable arp
  cable source-verify dhcp
  cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server on uBR7100
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
!   this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  speed 19200
line vty 0 4
  session-timeout 60
  login
!
```

```
ntp clock-period 17179977
ntp server 192.168.35.51
```

Additional References

For additional information related to DHCP, ToD, and TFTP Services for the CMTS Routers, refer to the following references:

Related Documents

Related Topic	Document Title
All-In-One Configuration	For information on how to configure a Cisco CMTS that acts as a Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP server in an "all-in-one configuration," see the following URL: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_configuration_example09186a0080134b34.shtml
DHCP Configuration	To configure the DHCP server beyond the minimum options given in this chapter, see the "Configuring DHCP" chapter in the "IP Addressing and Services" section of the *Cisco IOS IP and IP Routing Configuration Guide* , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html For information on all DHCP commands, see the "DHCP Commands" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
TFTP Server Command	For more information about the **tftp-server** command, see the "Configuring Basic File-Transfer Services" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf011.html
NTP or SNTP Configuration	For information on configuring the Cisco CMTS to use NTP or SNTP to set its system clock, see the "Performing Basic System Management" chapter in the "System Management" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* , at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html

Related Topic	Document Title
Cable Source Verify Feature	For a more detailed description of the cable source-verify command and how it can be used to prevent certain types of denial of service attacks, see the following Tech Note on Cisco.com: http://www.cisco.com/en/US/customer/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml
Calculating the Hexadecimal Value for DHCP Option 2	For information on how to calculate the hexadecimal time value that is used to set the DHCP Time Offset option (DHCP option 2), see the following URL: http://www.cisco.com/en/US/customer/tech/tk86/tk804/technologies_tech_note09186a0080093d76.shtml
Cisco DOCSIS Configurator Tool	For information on creating DOCSIS 1.1 configuration files, you can use the Cisco DOCSIS Configurator tool, which at the time of this document's publication is available at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference Guide,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Cisco uBR7100 Series Universal Broadband Router Documentation	*Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/installation/guide/hig7100.html *Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/configuration/guide/scg7100.html

Related Topic	Document Title
Cisco uBR7200 Series Universal Broadband Router Documentation	*Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/configuration/guide/cr72scg.html
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html

Standards

Standards[5]	Title
ANSI/SCTE 22-1 2002 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) (http://www.cablemodem.com)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification DOCSIS 1.1 (http://www.cablemodem.com)
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification (http://www.cablemodem.com)

5 Not all supported standards are listed.

MIBs

MIBs[6]	MIBs Link
• DOCS-CABLE-DEVICE-MIB (RFC 2669)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

6 Not all supported MIBs are listed.

RFCs

RFCs[7]	Title
RFC 868	Time Protocol
RFC 1350	The TFTP Protocol (Revision 2)
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DCHP Options and BOOTP Vendor Extensions
RFC 2349	TFTP Timeout Interval and Transfer Size Options
RFC 3046	DHCP Relay Agent Information Option
RFC4243	DHCP Relay Agent Information Sub-Option

7 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the DHCP, ToD, and TFTP Services for the CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 6: Feature Information for the DHCP, ToD, and TFTP Services for the CMTS Routers

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	11.3 NA	The **cable source-verify** and **ip dhcp** commands are now supported on the Cisco uBR7200 series routers.
DHCP, ToD, and TFTP Services	12.1(7)EC	The **cable helper-address** command is now supported.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.1(13)EC	The following commands are now supported on the Cisco IOS Release 12.1 EC train: **clear cable dhcp-giaddr-policy** **clear cable dhcp-lease-timer** **clear cable dhcp-server** The **cable source-verify** command has been expanded to include the **dhcp** keyword.
DHCP, ToD, and TFTP Services	12.1(13)EC	The Cisco uBR10012 series routers are now supported.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.1(13)EC	The Cisco uBR10012 series, Cisco uBR7200 series, and Cisco uBR7246VXR routers now support the above commands.
DHCP, ToD, and TFTP Services	12.1(13)EC 12.2(4)BC1	The **cable tftp-enforce** command is now supported.
DHCP, ToD, and TFTP Services	12.1(13)EC 12.2(4)BC1	The **cable source-verify** command has been expanded to include the **leasetimer** keyword.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.2(33)SCC	The cable source-verify dhcp command has been expanded to allow exclusion of MAC addresses

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.2(33)SCC	

Feature Name	Releases	Feature Information
		The **cable helper-address** command has been expanded to further specify where to forward DHCP packets based on origin from a cable modem, MTA, SIP, or other cable device. The **cable dhcp insert** command allows users to configure the CMTS to insert circuit ids into DHCP packets using option 82. DHCP

Feature Name	Releases	Feature Information
		servers can then detect cable modems and extract geographical information The **show cable modem** [*ip-address* | *mac-address*] **docsis** command is now supported
DHCP, ToD, and TFTP Servers	12.1(5)T	The **cable dhcp-giaddr** command was modified to support the **host**, **mta**, **ps**, and **stb** keywords

Feature Name	Releases	Feature Information
DHCP Source Address Validation	Cisco IOS XE Release 3.7.0S	The support for the DHCP Source Address Validation (SAV) feature was added. The following new commands were introduced: cable dhcp-giaddr policy cable dhcp-giaddr policy ip dhcp relay

Feature Name	Releases	Feature Information
DHCP Relay Agent Sub-option 82	12.2(15)BC2	Support was added for the DHCP Relay Agent Information Sub-option 82 feature. The following command was modified: cable dhcp-giaddr

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.

PART III

Downstream and Upstream Features

CHAPTER 8

Cable Modem Upstream RF Adaptation

First Published: June 13, 2011

The Cable Modem Upstream RF Adaptation feature uses per cable modem physical layer statistics to identify and automatically move cable modems to another logical upstream channel within the same physical port. This is to prevent unnecessary channel-wide parameter changes, which reduces throughput, disrupts traffic flow for all modems, and makes some modems to go offline in extreme cases.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Cable Modem Upstream RF Adaptation

- Multiple logical channels must be configured.
- Logical channels should be enabled per upstream.
- Logical channel 0 is the preferred primary logical channel, and logical channel 1 is the preferred secondary logical channel. This increases interoperability with other CMTS applications such as load balancing and upstream channel bonding.

The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 7: Cable Hardware Compatibility Matrix for Cable Modem Upstream RF Adaptation

Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V[8] • Cisco uBR-MC3GX60V[9]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC88V[10]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC88V

8 The Cisco UBR-MC20X20V cable interface line card has three variants—Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

9 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

10 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Cable Modem Upstream RF Adaptation

- Logical channel 1 cannot be part of an upstream bonding group.
- The Upstream Channel Bonding (USCB) feature coexists with the Cable Modem Upstream RF Adaptation feature; however, cable modems in the multiple transmits channel (MTC) mode are excluded.
- Cable modems that use the multiple receive channel (MRC) mode without MTC may participate in cable modem upstream RF adaptation because these cable modems can be moved using the dynamic channel change (DCC) method.
- Advanced spectrum management is not supported in multiple logical channel configurations.
- Dynamic channel-width configurations are not supported.
- A pair of logical upstream channels configured with a mix of DOCSIS modes (i.e. SCDMA on logical channel 0 and ATDMA on logical channel 1) is supported, however, the CMTS will request that the cable modem uses the initialization technique 1 for the DCC.

Information About Cable Modem Upstream RF Adaptation

The Cable Modem Upstream RF Adaptation feature moves a single cable modem or a group of cable modems to a more robust channel when a user-defined set of per cable modem PHY statistics does not meet a set of user-specified thresholds. Similarly, it releases a single cable modem or a group of cable modems from the secondary channel when the user-defined set of per cable modem PHY statistics exceeds a set of user-specified thresholds.

The following relocation methods are used while moving a cable modem to and from the secondary logical upstream channel:

- UCC for DOCSIS 1.0 cable modems.
- DCC initialization technique 2 for DOCSIS 1.1 and newer cable modems. Initialization technique 2 performs periodic ranging. The cable modem is kept online and allowed to start on the new channel with periodic ranging.
- DCC initialization technique 1 for any configuration where at least one logical channel uses the SCDMA DOCSIS mode. The initialization technique 1 broadcasts the initial ranging. The cable modem is kept online and re-registration is avoided, but this technique requires completion of initial ranging.

The following PHY statistics are used while moving a cable modem to and from the secondary logical upstream channel:

- Ranging burst Modulation Error Ratio (MER)
- Data burst MER for JIB3-based line cards
- Correctable and uncorrectable Forward Error Correction (FEC)

The cable modems to be relocated from the primary logical upstream channel to the secondary channel are marked as downgrade candidates. Similarly, the cable modems to be relocated from the secondary logical upstream channel to the primary channel are marked as upgrade candidates. Tracking individual cable modem statistics prevents a cable modem or a small group of cable modems from lowering the available bandwidth for the larger population of cable modems.

Following are the step-by-step timer-based events that occur during RF adaptation:

1. General timer event—The PHY statistics of the cable modems on the RF adapt-enabled channel are checked. The cable modems that fail or exceed the set threshold are flagged as either downgrade or upgrade candidates.
2. Candidate timer event—The PHY statistics of the cable modems that are flagged as downgrade or upgrade candidates are checked again to verify if the impairment still exists.
3. Relocation timer event—The cable modems that continue to fail or exceed the threshold are relocated.

After a line card switchover, the cable modems remain online on either the primary or secondary logical upstream channel depending on the state of the cable modem prior to the switchover. The upgrade and downgrade candidate cable modems, and the cable modem movement history from primary to secondary logical upstream channel and vice versa are not retained after a line card switchover. The Cable Modem Upstream RF Adaptation feature is not affected by a PRE switchover and the candidate information and history is retained during a PRE switchover.

The Cable Modem Upstream RF Adaptation feature is disabled by default. For information about how to enable this feature, see How to Configure Cable Modem Upstream RF Adaptation, on page 193.

Related CMTS Software Features

The Cable Modem Upstream RF Adaptation feature via spectrum management integrates with and leverages from the following CMTS software features:

- Multiple Logical Channels, on page 192
- CMTS PHY Measurement, on page 193

Multiple Logical Channels

The ability to use a multiple logical channel configuration to relocate cable modems with PHY impairments is a key capability of the Cable Modem Upstream RF Adaptation feature. In a cable modem upstream RF adaptation configuration, the logical channels are used as:

- Logical Channel 0—This is the default primary logical channel that cable modems registers on. The primary logical channel should be configured with performance options such as 64 QAM modulation profile irrespective of the index value.
- Logical Channel 1—This is the default secondary logical channel. The secondary logical channel should be configured with robust options, such as QPSK-based modulation profile irrespective of the index value.

You can configure the primary and secondary logical channel. When multiple logical channels are configured, the upstream-related commands are categorized into physical port level and logical channel level groups. Logical channel level commands use the format of **cable upstream** *port logical-channel-index*, where *port* denotes the physical port number, and *logical-channel-index* denotes the logical channel index number.

The following logical channel-level configuration options have an impact on the Cable Modem Upstream RF Adaptation feature:

- DOCSIS mode. In the case of SCDMA, change in parameters like codes-per-minislot may also impact robustness.
- Modulation profile.

- Equalization-coefficient (that is pre-equalization).

For more details on the Multiple Logical Channel feature, see S-CDMA and Logical Channel Support on the Cisco CMTS Routers .

CMTS PHY Measurement

The CMTS PHY measurements collected on a per cable modem basis is used during RF adaptation. For a cable modem upstream RF adaptation, the MER (also referred to as Signal-to-noise Ratio [SNR]), and FEC (both correctable and uncorrectable) measurements provide an accurate indication about the effect of any PHY impairments on a single cable modem.

The Cable Modem Upstream RF Adaptation feature uses the following thresholds:

- rf-adapt—Sets the RF adaptation percentage threshold.
- snr-profiles—Specifies the MER (SNR) threshold in dB.
- hysteresis—Specifies the hysteresis value.
- corr-fec—Specifies the allowable number of correctable FEC errors for the upstream.
- uncorr-fec—Specifies the allowable number of uncorrectable FEC errors for the upstream.

Note All the above thresholds are configured at the physical port level to ensure that the same collection of thresholds is used for both upgrade and downgrade.

How to Configure Cable Modem Upstream RF Adaptation

This section describes how to configure a physical upstream and its associated logical channels for cable modem upstream RF adaptation.

Before You Begin

Multiple logical channels must be configured.

Restriction The cable modem upstream RF adaptation is not applicable for modems that are registered in MTC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rf-adapt timer general** *time* **Example:** `Router(config)# cable rf-adapt timer general 1`	(Optional) Sets the timer for cable modem upstream RF adaptation. • **general** *time*—Specifies the period when the RF adaptation process examines the physical layer statistics of all modems on RF adaptation-enabled upstream channels. The valid range is from 1 to 300 seconds.
Step 4	**cable rf-adapt timer candidate** *time* **Example:** `Router(config)# cable rf-adapt timer candidate 2`	(Optional) Sets the timer for cable modem upstream RF adaptation. • **candidate** *time*—Specifies the period when the RF adaptation process examines the physical layer statistics of modems flagged as downgrade or upgrade candidates, or both. The valid range is from 1 to 300 seconds.
Step 5	**cable rf-adapt timer relocation** *time* **Example:** `Router(config)# cable rf-adapt timer relocation 300`	(Optional) Sets the timer for cable modem upstream RF adaptation. • **relocation** *time*—Specifies the period when the RF adaptation process performs a single relocation of a candidate modem from its current upstream channel to the appropriate destination. The valid range is from 1 to 300 seconds.
Step 6	**interface cable** {*slot*/*cable-interface-index* | *slot*/*subslot*/*cable-interface-index*} **Example:** `Router(config)# interface cable 8/0/0`	Enters interface configuration mode. • *slot*—Slot where the line card resides. ◦ Cisco uBR7225VXR router—The valid value is 1 or 2. ◦ Cisco uBR7246VXR router—The valid range is from 3 to 6. ◦ Cisco uBR10012 router—The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. The valid subslot is 0 or 1. • *cable-interface-index*—Downstream port of the Cisco uBR10-MC5X20 and Cisco uBR-MC88V line cards, or MAC domain index of the Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards. ◦ Cisco uBR7225VXR and Cisco uBR7246VXR routers—The valid port value is 0 or 1. ◦ Cisco uBR10012 router—The valid range for the Cisco UBR-MC20X20V and Cisco uBR-MC5X20 line cards is from 0 to 4. The valid range for the Cisco uBR-MC3GX60V line card is from 0 to 14.

	Command or Action	Purpose
Step 7	**cable upstream***port***max-logical-chans** *code* **Example:** `Router(config-if)# cable upstream 0 max-logical-chans 2`	Enables multiple logical channels on the physical upstream channel intended for RF adaptation. • *port* —Upstream port. The valid range is from 0 to 3. • *code* —Number of logical channels per port. The valid values are 1 and 2.
Step 8	**cable upstream** *port* **rf-adapt** **Example:** `Router(config-if)# cable upstream 0 rf-adapt`	Enables RF adaptation on the physical upstream channel. • *port*—Upstream port. The valid range is from 0 to 3.
Step 9	**cable upstream** *port* **threshold rf-adapt** *threshold1-in-percent* **Example:** `Router(config-if)# cable upstream 0 threshold rf-adapt 25`	(Optional) Sets the RF adaptation percentage threshold. • *port* —Upstream port. The valid range is from 0 to 3. • **rf-adapt**—Specifies the ratio of candidate cable modems to total number of upstream cable modems, which disables further RF adaptation. • *threshold1-in-percent*—RF adapt disable threshold in percentage. The valid range is from 1 to 50. **Note** You can bypass the RF adapt disable threshold by setting it to 0.
Step 10	**cable upstream***port***thresholdsnr-profiles***snr-threshold1 snr-threshold2* **Example:** `Router(config-if)# cable upstream 0 threshold snr-profiles 25 0`	(Optional) Specifies the MER (SNR) threshold in dB. • *snr-threshold1*—MER (SNR) threshold for the primary modulation profile specified for the upstream. The valid range is from 5 to 35 dB, with a default value of 25 dB. **Note** You can bypass the primary MER (SNR) threshold (snr-threshold1-in-db) by setting it to 0. • *snr-threshold2*—MER (SNR) threshold for the secondary modulation profile specified for the upstream. The valid range is from 5 to 35 dB, with a default value of 25 dB. For the Cable Modem Upstream RF Adaptation feature, it is recommended to set this value to 0. **Note** *snr-threshold2* is ignored by the Cable Modem Upstream RF Adaptation feature.
Step 11	**cable upstream***port***thresholdhysteresis***hysteresis-value* **Example:** `Router(config-if)# cable upstream 0 threshold hysteresis 3`	(Optional) Specifies the hysteresis value. • *hysteresis-value*—Hysteresis value. The valid range is from 0 to 10 dB, with a default value of 3 dB. **Note** You can bypass the hysteresis threshold by setting the value to 0.

	Command or Action	Purpose
Step 12	**cable upstream***port***threshold corr-fec***fec-corrected* **Example:** `Router(config-if)# cable upstream 0 threshold corr-fec 2`	(Optional) Specifies the allowable number of correctable FEC errors for the upstream. • *fec-corrected* —Allowable number of correctable FEC errors for the upstream, given as a percentage of total packets received on the upstream during the polling period. It is given as a percentage of total packets received on the upstream during the polling period. The valid range is from 1 to 30 percent, with a default value of 3 percent. **Note** You can bypass the corr-fec threshold by setting the value to 0.
Step 13	**cable upstream***port***threshold uncorr-fec***fec-uncorrected* **Example:** `Router(config-if)# cable upstream 0 threshold uncorr-fec 10`	(Optional) Specifies the allowable number of uncorrectable FEC errors for the upstream. • *fec-uncorrected* —Allowable number of uncorrectable FEC errors for the upstream, given as a percentage of total packets received on the upstream during the polling period. The valid range is from 1 to 30 percent of total packets, with a default of 1 percent. **Note** You can bypass the uncorr-fec threshold by setting the value to 0.
Step 14	**cable upstream** *port logical-channel-index* **rf-adapt** [**primary** | **secondary**] **Example:** `Router(config-if)# cable upstream 0 0 rf-adapt primary`	(Optional) Specifies the primary upstream logical channel and the secondary upstream logical channel. • *port* —Upstream port. The valid range is from 0 to 3. • *logical-channel-index* —Logical channel index. The valid values are 0 and 1. • **primary**—Sets the logical channel as primary for RF adaptation. By default, the logical channel 0 is primary. • **secondary**—Sets the logical channel as secondary for RF adaptation. By default, the logical channel 1 is secondary. **Note** When you set the primary channel, the secondary channel is automatically set.
Step 15	**no cable upstream** *portlogical-channel-index* **shutdown** **Example:** `Router(config-if)# no cable upstream 0 1 shutdown`	Performs a “no shutdown” on logical channel 1.

	Command or Action	Purpose
Step 16	**end** **Example:** `Router(config-if)# end`	Exits the interface configuration mode and returns to privileged EXEC mode.

What to Do Next

If you want to customize multiple logical channels, see S-CDMA and Logical Channel Support on the Cisco CMTS Routers.

Troubleshooting Tips

Following are some scenarios that you may encounter while configuring or after configuring the Cable Modem Upstream RF Adaptation feature. Follow the recommended action to resolve these issue.

Cable Modem Does Not Downgrade to the Secondary Logical Channel

Problem A cable modem with PHY statistics less than the user-specified threshold is not downgraded to the secondary logical channel.

- **Possible Cause** The RF adaptation downgrade threshold has been met.
- **Possible Cause** The RF adaptation downgrade threshold is exceeded while the cable modem is still on the downgrade candidate list.
- **Possible Cause** The RF adaptation downgrade threshold is exceeded after a group of cable modems are moved to the secondary logical channel.

Solution Contact Cisco Technical Assistance Center (TAC).

Cable Modem Does Not Upgrade to the Primary Logical Channel

Problem A cable modem with PHY statistics greater than the user-specified threshold is not upgraded to the primary logical channel.

- **Possible Cause** The cable modem was upgraded or downgraded five times.
- **Possible Cause** The SNR has not improved beyond the threshold and the hysteresis value.

Solution You can delete the cable modem history from the CMTS database using the **clear cable modem delete** command.

Verifying Cable Modem Upstream RF Adaptation

Command	Purpose
show cable rf-adapt downgrade-candidates	To verify the downgrade candidate cable modems.
show cable rf-adapt upgrade-candidates	To verify the upgrade candidate cable modems.
show cable modem rf-adapt	To verify the RF adaptation history

Configuration Examples for Cable Modem Upstream RF Adaptation

This section provides configuration examples for the Cable Modem Upstream RF Adaptation feature:

Example: Configuring Cable Modem Upstream RF Adaptation on the Cisco uBR10012 Router

The following example shows how to configure the Cable Modem Upstream RF Adaptation feature on the Cisco uBR10012 router.

```
!
interface Cable8/0/0
 load-interval 30
 downstream Modular-Cable 1/1/0 rf-channel 0 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 700
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 13000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 max-logical-chans 2
 cable upstream 0 threshold snr-profiles 20 0
 cable upstream 0 threshold corr-fec 0
 cable upstream 0 threshold uncorr-fec 0
 cable upstream 0 threshold rf-adapt 0
 cable upstream 0 rf-adapt
 cable upstream 0 0 docsis-mode scdma
 cable upstream 0 0 spreading-interval 16
 cable upstream 0 0 codes-per-minislot 16
 cable upstream 0 0 active-codes 112
 cable upstream 0 0 range-backoff 3 6
 cable upstream 0 0 modulation-profile 321
 cable upstream 0 0 attribute-mask 20000000
 no cable upstream 0 0 shutdown
 cable upstream 0 1 docsis-mode atdma
 cable upstream 0 1 minislot-size 1
 cable upstream 0 1 range-backoff 3 6
 cable upstream 0 1 modulation-profile 223
 cable upstream 0 1 attribute-mask 20000000
 no cable upstream 0 1 shutdown
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
```

```
 cable upstream 1 frequency 20000000
 cable upstream 1 channel-width 3200000 3200000
 cable upstream 1 load-balance group 80
 cable upstream 1 docsis-mode scdma
 cable upstream 1 spreading-interval 16
 cable upstream 1 codes-per-minislot 4
 cable upstream 1 active-codes 112
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 321
 cable upstream 1 attribute-mask 20000000
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 frequency 26400000
 cable upstream 2 channel-width 3200000 3200000
 cable upstream 2 power-level 1
 cable upstream 2 load-balance group 80
 cable upstream 2 docsis-mode scdma
 cable upstream 2 spreading-interval 16
 cable upstream 2 codes-per-minislot 4
 cable upstream 2 active-codes 112
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 321
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 frequency 32600000
 cable upstream 3 channel-width 3200000 3200000
 cable upstream 3 power-level 1
 cable upstream 3 load-balance group 80
 cable upstream 3 docsis-mode scdma
 cable upstream 3 spreading-interval 16
 cable upstream 3 codes-per-minislot 4
 cable upstream 3 active-codes 112
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 321
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
 cable sid-cluster-group num-of-cluster 2
 cable sid-cluster-switching max-request 1
...
...
```

Example: Configuring Cable Modem Upstream RF Adaptation on the Cisco uBR7200 Router

The following example shows how to configure the Cable Modem Upstream RF Adaptation feature on the Cisco 7200 router.

```
!
interface Cable1/1
 load-interval 30
 downstream Integrated-Cable 1/1 rf-channel 0-3 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 2
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 20000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 max-logical-chans 2
 cable upstream 0 threshold snr-profiles 26 0
 cable upstream 0 threshold corr-fec 5
 cable upstream 0 threshold uncorr-fec 2
 cable upstream 0 threshold hysteresis 4
 cable upstream 0 threshold rf-adapt 0
 cable upstream 0 rf-adapt
 cable upstream 0 0 docsis-mode atdma
 cable upstream 0 0 minislot-size 4
 cable upstream 0 0 range-backoff 3 6
 cable upstream 0 0 modulation-profile 221
```

```
cable upstream 0 0 attribute-mask 20000000
no cable upstream 0 0 shutdown
cable upstream 0 1 docsis-mode atdma
cable upstream 0 1 minislot-size 4
cable upstream 0 1 range-backoff 3 6
cable upstream 0 1 modulation-profile 222
cable upstream 0 1 attribute-mask 20000000
no cable upstream 0 1 shutdown
no cable upstream 0 shutdown
cable upstream 1 connector 5
cable upstream 1 frequency 26600000
cable upstream 1 channel-width 3200000 3200000
cable upstream 1 docsis-mode atdma
cable upsteram 1 minislot-size 4
cable upstream 1 range-backoff 3 6
cable upstream 1 modulation-profile 321
cable upstream 1 attribute-mask 20000000
no cable upstream 1 shutdown
cable upstream 2 connector 6
cable upstream 2 frequency 30000000
cable upstream 2 channel-width 3200000 3200000
cable upstream 2 docsis-mode atdma
cable upsteram 2 minislot-size 4
cable upstream 2 range-backoff 3 6
cable upstream 2 modulation-profile 221
cable upstream 2 attribute-mask 20000000
no cable upstream 2 shutdown
cable upstream 3 connector 7
cable upstream 3 frequency 33500000
cable upstream 3 channel-width 3200000 3200000
cable upstream 3 docsis-mode atdma
cable upsteram 3 minislot-size 4
cable upstream 3 range-backoff 3 6
cable upstream 3 modulation-profile 221
cable upstream 3 attribute-mask 20000000
no cable upstream 3 shutdown
end
```

Example: Non-Default Timer Configuration

The following example shows how to configure non-default timer configuration.

```
Router# show running-config | in timer
cable rf-adapt timer general 60
cable rf-adapt timer candidate 15
cable rf-adapt timer relocation 5
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CMTS cable commands	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.htmlCisco IOS CMTS Cable Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Modem Upstream RF Adaptation

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

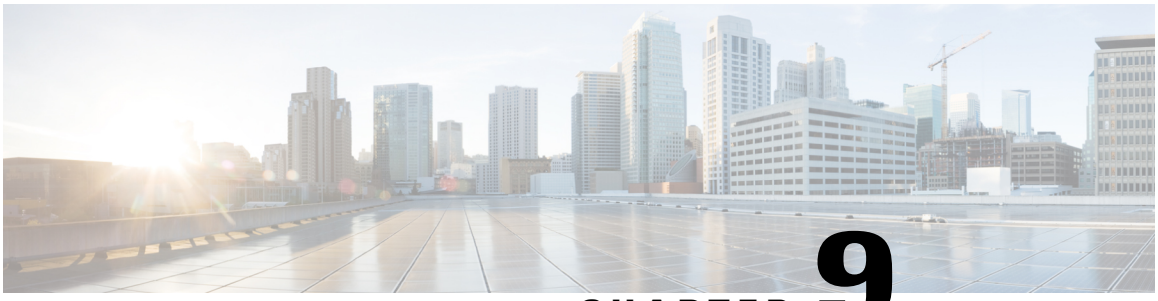
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 8: Feature Information for Cable Modem Upstream RF Adaptation

Feature Name	Releases	Feature Information
Cable Modem Upstream RF Adaptation	12.2(33)SCF	

Feature Name	Releases	Feature Information
		The Cable Modem Upstream RF Adaptation feature uses the per cable modem physical layer statistics to identify and automatically move cable modems to another logical upstream channel within the same physical port to prevent unnecessary channel-wide parameter changes. In Cisco IOS Release 12.2(33)SCF, this feature was introduced on the Cisco uBR10012 router and Cisco uBR7200 series routers. The following sections provide information about this feature: • Information About Cable Modem Upstream RF Adaptation, on page 191 • How to Configure Cable Modem Upstream RF Adaptation, on page 193 • Verifying Cable Modem Upstream RF Adaptation, on page 198 • Configuration Examples for Cable Modem Upstream RF Adaptation, on page 198 The following commands were introduced or modified: **cable rf-adapt timer, cable upstream rf-adapt(logical channel), cable upstream rf-adapt, cable upstream threshold rf-adapt, show cable modem rf-adapt, show cable rf-adapt, cable upstream threshold hysteresis, cable upstream threshold, show cable modem, show cable modem access-group, show cable modem calls, show cable modem connectivity, show cable modem counters, show cable modem docsis version, show cable modem domain-name, show cable modem errors, show cable**

Feature Name	Releases	Feature Information
		modem flap, show cable modem ipv6, show cable modem mac, show cable modem maintenance, show cable modem offline, show cable modem phy, show cable modem primary channel, show cable modem registered, show cable modem rogue, show cable modem summary, show cable modem type, show cable modem unregistered, show cable modem vendor, show cable modem wideband.



CHAPTER 9

Configuring Downstream Cable Interface Features on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: May 12, 2009

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The cable interface in the Cisco universal broadband routers serves as the cable TV radio frequency (RF) interface, supporting downstream and upstream signals. The downstream signal is output as an intermediate-frequency (IF) signal suitable for use with an external upconverter. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determines the combination of cable interfaces, network uplink line cards, and other components that you should use.

The Cisco IOS software command-line interface (CLI) can be used to configure the Cisco cable interface line card for correct operation on the hybrid fiber-coaxial (HFC) cable network. This chapter provides a configuration summary for the various downstream cable interface features available on a Cisco CMTS router. Details about some of these features can be found in other chapters of this book.

Note The configuration commands and examples in this chapter may show slot numbering or references to either Cisco uBR7200 series or Cisco uBR10012 Universal Broadband Routers. However, the features can be configured on either platform. Use the slot numbering appropriate for your CMTS router configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring Downstream Cable Interfaces on the Cisco CMTS Routers

The configuration of downstream cable interface features is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table below shows the hardware compatibility prerequisites for this feature.

Table 9: Configuring Downstream Cable Interfaces on the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE-2 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Note In most applications, default values for the commands used in these configuration steps are adequate to configure the Cisco CMTS router. You do not need to specify individual parameters unless you want to deviate from system defaults.

Activating Downstream Cable Address Resolution Protocol Requests

This configuration is required. Address Resolution Protocol (ARP) is an Internet protocol used to map IP addresses to MAC addresses on computers and other equipment installed in a network. You must activate ARP requests on the cable interface so that the Cisco uBR10000 series CMTS can perform IP address resolution on the downstream path.

Note The default values for the commands used in this configuration step are adequate in most cases to configure the Cisco uBR7200 series CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface cable5/0** **Example:** `Router(config)# interface cable5/0`	Enters cable interface configuration mode. In this example, the interface is downstream port 0 on the cable interface card installed in slot 1 of the Cisco uBR7200 series CMTS.
Step 4	**cable arp** **Example:** `Router(config-if)# cable arp`	Enables ARP. This is the default.

What to Do Next

To verify that cable ARP is activated, enter the **more system:running-config** command and look for the cable interface configuration information. If ARP is activated, it does not appear in this output. If ARP is deactivated, it appears in the output as

```
no cable arp
.

Router# more system:running-config
Building configuration...

Current configuration:
!
interface cable5/0
ip address 1.1.1.1 255.255.255.0
 no keepalive
 no cable arp
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, verify that you entered the correct port and cable interface line card slot number when you activated ARP and when you entered the **show interface cable** command.

Activating Downstream Ports

To activate a downstream port on a Cisco uBR7200 series cable interface card for digital data transmissions over the HFC network, complete the steps in the following table.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable5/0** **Example:** `Router(config)# interface cable5/0`	Enters cable interface configuration mode. In this example, the interface is downstream port 0 on the cable interface card installed in slot 1 of the Cisco uBR7200 series CMTS.
Step 4	Enter the following commands: • **cable downstream if-output** • **no cable downstream if-output** **Example:** `Router(config-if)# cable downstream if-output` `Router(config-if)# no cable downstream if-output`	Activates downstream digital data from the Cisco uBR7200 series router. Deactivates downstream digital data. This command mutes the IF output of the cable interface card and shuts down the interfaces.
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Places the downstream port in the "admin up" state.
Step 6	**end** **Example:** `Router(config-if)# end` `Router#` `%SYS-5-CONFIG_I: Configured from console by console`	Returns to privileged EXEC mode. This message is normal and does not indicate an error.

What to Do Next

To determine if the downstream carrier is active (up), enter the **show controllers cable** command for the downstream port that you just configured. For National Television Standards Committee (NTSC) 6 MHz operations, see the following example:

```
Router# show controllers cable5/0 downstream

Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
```

Assigning the Downstream Channel ID

To assign a numeric channel ID to the downstream port on the Cisco cable interface line card, use the following command in cable interface configuration mode.

```
Router(config-if)# cable downstream channel-id id
```

Note For Cisco IOS Release 12.2(33)SCB and later releases, the acceptable range is 1 to 255 (0 is reserved for network management) and for releases prior to Cisco IOS Release 12.2(33)SCB, the acceptable range is 0 to 255.

Note The **cable downstream channel-id** command must be used with the following command:
`cable downstream frequency 54000000-1000000000 broadcast frequency - h`

These commands are used in instances where you want to send multiple downstream frequencies to a single region that contains CMs that can connect only to upstream ports on the same cable interface line card. You must configure unique channel IDs for each downstream that any CM is capable of receiving. The downstream frequency setting must match the setting on the upconverter.

Caution After defining unique downstream IDs, test the CMs for correct operation. Cisco recommends that when using this feature, you re-test each subsequent software release of CM code to verify correct operation and to ensure reasonable acquisition time for new installations. Failure to use these commands in conjunction or to test the involved CMs can result in customer service outages of indefinite duration.

Verifying the Downstream Channel ID

To verify the downstream channel ID, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream

Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 1
```

Traffic Shaping

Traffic shaping basically uses queues to limit data surges that can congest a network. The data is buffered and then sent into the network in regulated amounts to ensure that the traffic fits within the expected traffic envelope for the particular connection.

Traffic shaping reduces the chance that information must be retransmitted to hosts on the cable plant. When cable modems (CMs) have rate limits established, the CMTS typically drops data packets to enforce the rate limit. Dropping packets from the requesting CM causes the host sending the information to retransmit its information, which wastes bandwidth on the network. If both hosts sending and requesting information are on the cable plant, the upstream bandwidth is wasted as well.

Traffic shaping allows the CMTS to perform upstream and downstream rate limiting on the DOCSIS upstream and downstream channels. Rate limiting restricts the data rate to and from a CM; the MAC scheduler supports traffic-shaping capabilities for downstream and upstream traffic. Rate limiting ensures that no single CM consumes all of the channel bandwidth and allows a CMTS administrator to configure different maximum data rates for different subscribers. Subscribers requiring higher sustained rates and willing to pay for higher rates can be configured with higher sustained rate limits in their CM DOCSIS configuration file over regular subscribers, who pay less and get lower rate limits.

Each time a packet belonging to a flow is transmitted on an output channel, the token-bucket policer function checks the rate limit status of the flow, passing the following parameters:

- Token bucket maximum sustained rate in bits per millisecond.
- Token bucket depth (maximum transmit burst) in bits.
- Length of current packet to be sent in bits.
- Pointer to the flow's token bucket.
- Pointer to the flow's token bucket last update time stamp.
- Variable to return the milliseconds buffering delay in case the packet needs to be shaped.
- Maximum buffering delay that the subsequent traffic shaper can handle in milliseconds.

Every flow has its own shaping buffer where rate-exceeded packets are typically held back in first-in/first-out (FIFO) order for later releases transmission.

Tip Token bucket policing with shaping is the per-upstream default rate limiting setting at the CMTS. Shaping can be enabled or disabled for the token-bucket algorithm.

Downstream Traffic Shaping

The CMTS supports basic downstream traffic shaping by effecting data rate limiting on a per-modem basis. A downstream traffic shaping feature called downstream rate limiting with type of service (ToS) bits extends that capability by allowing the CMTS administrator to configure the ToS byte to calculate the data rate for a specified flow.

Downstream rate limiting with ToS bits enables you to partition downstream traffic for a CM into multiple classes of service and multiple data rates by using the three precedence bits in the ToS byte in the IP header to specify a class of service assignment for each packet. Those packets with the precedence bit set in the ToS field are given higher priority. Using the ToS byte, you can calculate the data rate for a specified flow, in addition to the data rate configured on a per-CM basis. By specifying a maximum data rate for a particular ToS, you can override the common maximum downstream data rate.

The administrator can override the maximum common downstream data rate limits by configuring the ToS byte.

Packets that contain ToS bytes that have not been configured for downstream data rates continue to use the common data rate limits.

Configuring Downstream Rate Limiting and Traffic Shaping

To configure downstream traffic shaping, use the following command in cable interface configuration mode.

Command	Purpose
`Router(config-if)# [no] cable downstream rate-limit token-bucket [shaping] weighted-discard [expwt <n>]`	Enables or disables rate limiting and traffic shaping on the downstream of a cable interface.

Note Using Cisco IOS Release 12.0(5)T1 or higher, the software adds downstream calendar queuing routines and grant shaping application of the calendar queues.

Note Effective with Cisco IOS Release 12.2(33)SCF, the **cable downstream rate-limit** command is not supported for Cisco uBR-MC88U line card in Cisco IOS software.

Details for key command usage are provided below:

- To enable rate limiting on the given downstream port using the token bucket policing algorithm, issue the **cable downstream rate-limit token-bucket** command.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with traffic shaping, issue the **cable downstream rate-limit token-bucket shaping** command.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with a specific traffic shaping time granularity, issue the **cable downstream rate-limit token-bucket shaping granularity 8** command. Acceptable values are 1, 2, 4, 8, or 16 msecs.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with a specific maximum traffic shaping buffering delay, issue the **cable downstream rate-limit token-bucket shaping granularity 8** command. Acceptable values are 128, 256, 512, or 1028 msecs.
- To remove rate limiting on the given downstream port, issue the **cable downstream rate-limit token-bucket** command.
- To enable rate limiting on the given downstream port using a weighted packet discard policing algorithm and to assign a weight for the exponential moving average of loss rate value, issue the **cable downstream rate-limit weighted-discard 3** command. Acceptable values are 1 to 4.

Setting the Downstream Helper Address

Specify an IP address of a Dynamic Host Configuration Protocol (DHCP) server where User Datagram Protocol (UDP) broadcast packets will be sent. You can specify a DHCP server for UDP broadcast packets from cable interfaces, and a DHCP server for UDP broadcast packets from hosts. To set a downstream helper address, use the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cable helper-address 10.***x.x.x* **cable-modem** **Example:** `Router(config-if)# cable helper-address 10.x.x.x cable-modem`	Set the downstream helper address to the DHCP server at IP address 10.*x.x.x* for UDP broadcast packets from cable modems. **Note** Use the IP address of the DHCP server. Both 10.*x.x.x* and 172.56.*x.x* are private ranges.
Step 2	**cable helper-address 172.56.** *x.x***host** **Example:** `Router(config-if)# cable helper-address 172.56.x.x host`	Set the downstream helper address to the DHCP server at IP address 172.56.*x.x* for UDP broadcast packets from hosts.

Verifying the Downstream Helper Address

To verify the downstream helper address setting, enter the **show running-config** command and look for cable helper-address in the cable interface configuration information:

```
Router# show running-config

Building configuration...
Current configuration:
!
interface cable5/0
ip address 10.254.254.254 255.0.0.0
 no ip directed-broadcast
 cable helper-address 192.168.1.1
 no keepalive
```

Perform these steps if you are having difficulty with verification:

Step 1 Check the cables, upconverters, RF levels, and frequencies if the cable interfaces do not find a downstream signal.

Step 2 Check the cables, RF levels, and upstream frequencies, and enter a no shut command if the cable interfaces find a downstream signal, but not an upstream signal.

Step 3 Check the provisioning servers.

- Ping the DHCP server using the source IP address option—the primary IP address of a cable interface.
- Check IP routing if the cable interfaces acquire an RF upstream and downstream lock, but do not stay up.

Step 4 Check DHCP options and the IP address of the Time-of-Day (ToD) server:

- Ping the ToD server using the source IP address option.
- Check IP routing.
- Verify that the TFTP filename is correct.
- Verify that the TFTP file is in the correct directory on the TFTP server.

- Ensure that the TFTP file has read privileges.
- Ping the TFTP server using the source IP address option, and check IP routing if the cable interfaces acquire an RF and a DHCP, but fail on ToD or TFTP.

Setting the Downstream Interleave Depth

Set the interleave depth for the downstream port on the Cisco cable interface line card. A higher interleave depth provides more protection from bursts of noise on the HFC network; however, it increases downstream latency.

Note The valid values are 8, 16, 32 (default), 64, and 128.

To set the downstream interleave depth in milliseconds, use the following command in cable interface configuration mode:

```
Router(config-if)# cable downstream interleave-depth {8 | 16 | 32 | 64 | 128}
```

Verifying the Downstream Interleave Depth

To verify the downstream interleave depth setting, enter the **show controllers cable** command for the downstream port you have just configured:

```
Router# show controllers cable5/0 downstream

Cable5/0 Downstream is up
 Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that the downstream carrier is active, using the **cable downstream if-output** command.

Setting the Downstream Modulation

To set the downstream modulation, define the speed in symbols per second at which data travels downstream to the subscriber's CM. A symbol is the basic unit of modulation. Quadrature Phase Shift Key (QPSK) encodes

2 bits per symbol, Quadrature Amplitude Modulation (QAM) -16 encodes 4 bits per symbol, QAM-64 encodes 6 bits per symbol, and QAM-256 encodes 8 bits per symbol.

Note Setting a downstream modulation rate of QAM-256 requires approximately a 6 dB higher signal-to-noise ratio (SNR) than QAM-64 at the subscriber's cable interface. If your network is marginal or unreliable at QAM-256, use the QAM-64 format instead. Also, consider the significance of your data.

To set the downstream modulation, use the following command in cable interface configuration mode. The standard DOCSIS modulation rate (and the Cisco default) is QAM-64.

```
Router(config-if)# cable downstream modulation 64qam
```

Verifying the Downstream Modulation

To verify the downstream modulation setting, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream

Cable5/0 Downstream is up
 Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers

Step 5 Verify that the downstream carrier is active, using the **cable downstream if-output** command

Step 6 Verify that you have selected the default if you are not certain about the modulation rate needed.

Setting the Downstream MPEG Framing Format

The MPEG framing format must be compatible with DOCSIS specifications at:

http://www.cablelabs.com/cablemodem/ and your local cable plant operations.

Tip Annex B is the DOCSIS MPEG framing format standard for North America.

Note Annex B framing format is automatically set when configuring Cisco cable interface line cards. The cable interface line card's downstream ports and the connected CMs on the network must be set to the same MPEG framing format and must support DOCSIS operations as appropriate.

The following command appears in the Cisco uBR7200 series router configuration file to designate Annex B operation. This command sets the downstream MPEG framing format.

```
Router(config-if)# cable downstream annex {B}
```

Verifying the Downstream MPEG Framing Format

To verify the downstream MPEG framing format setting, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream

Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 1
```

Setting Downstream Traffic Shaping

Downstream traffic shaping enables you to use the token bucket policing algorithm with traffic shaping options or the weighted discard algorithm to buffer, shape, or discard packets that exceed a set bandwidth. Downstream traffic shaping is disabled by default.

To enable downstream traffic shaping for a downstream port on a Cisco cable interface line card, use one of the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cable downstream rate-limit token-bucket** [**shaping** [**granularity** *msec* | **max-delay** *msec*]	Enables traffic shaping on the downstream port using the token bucket policing algorithm. With this command, the Cisco uBR7200 series router automatically drops packets that are in violation of the allowable bandwidth.
	Example: `Router(config-if)# cable downstream rate-limit token-bucket`	Enables traffic shaping on the downstream port using the token bucket policing algorithm with traffic shaping.
	`Router(config-if)# cable downstream rate-limit token-bucket shaping`	Enables traffic shaping on the downstream port using the token bucket policing algorithm with specific traffic shaping time granularity. Acceptable values are 1, 2, 4, 8, or 16 milliseconds.
	`Router(config-if)# cable downstream rate-limit token-bucket shaping granularity 8`	Enables traffic shaping on the downstream port using the token bucket policing algorithm with specific maximum traffic shaping buffering delay. Acceptable values are 128, 256, 512, or 1028 milliseconds.
	`Router(config-if)# cable downstream rate-limit token-bucket shaping max-delay 256`	
Step 2	**cable downstream rate-limit weighted-discard** *exp-weight*	Enables traffic shaping on the downstream port using the weighted discard algorithm and assigns a weight for the exponential moving average of the loss rate. Acceptable values are 1 to 4.
	Example: `Router(config-if)# cable downstream rate-limit weighted-discard 3`	

	Command or Action	Purpose
Step 3	**end** **Example:** `Router(config-if)# end`	Exits back to privileged EXEC mode so that you can verify the steps.

Verifying Downstream Traffic shaping

To determine if downstream traffic shaping is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If downstream traffic shaping is configured and enabled, a traffic shaping entry appears in the output. If downstream traffic shaping is disabled, no traffic shaping entry appears.

```
Router# show running-config
Building configuration...
Current configuration:
!
interface cable5/0
ip address 10.254.254.254 255.0.0.0
no ip directed-broadcast
cable helper-address 192.168.1.1
no keepalive
cable downstream annex B
cable downstream modulation 64qam
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected the default if you are not certain about the modulation rate needed.

Step 6 Verify that the downstream carrier is active using the **cable downstream if-output** command.

Activating Host-to-Host Communication (Proxy ARP)

Cable proxy ARP allows a Cisco CMTS router to issue cable ARP requests on behalf of CMs on the same cable network subnet.

Note Because the downstream and upstreams are separate interfaces, modems cannot directly perform ARP with other modems on the cable plant.

Note The default values for the commands used in this configuration task are adequate in most cases to configure the Cisco CMTS routers.

Activating Cable Proxy ARP Requests

This configuration is optional. To activate cable proxy ARP for host-to-host communications, use the following command in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable proxy-arp`	Enables proxy ARP on the cable interface. This is the default.

Verifying Cable Proxy ARP Requests

To verify if cable proxy ARP has been activated or deactivated, enter the **more system:running-config** command and look for the cable interface configuration information. If cable proxy ARP has been activated, it does not appear in the output. If cable proxy ARP has been deactivated, it appears in the output as no cable proxy-arp.

```
Router# more system:running-config

Building configuration...

Current configuration:
!
interface cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 no cable proxy-arp
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, make sure that you entered the correct port and cable interface line card slot number when you activated cable proxy ARP.

Activating Packet Intercept Capabilities

This configuration is optional. To activate packet intercept functionality, use the following commands in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable intercept` *xxxx.xxxx.xxxx*	Specifies a MAC address on the cable network for which interception capabilities are to be activated. There is a limit of 10 MAC addresses.
`Router(config-if)# no cable intercept` *xxxx.xxxx.xxxx*	Disables interception after it is enabled.

Configuring Payload Header Suppression and Restoration

This configuration is optional. Payload Header Suppression (PHS) is a new feature in the DOCSIS1.1 MAC driver. The PHS feature is used to suppress repetitive or redundant portions in packet headers before transmission on the DOCSIS link. The upstream receive driver is now capable of restoring headers suppressed by CMs, and the downstream driver is capable of suppressing specific fields in the packet header before forwarding the frame to the CM.

Command	Purpose
show interface cable *x/0/0* **service-flow [***sfid***] phs**	Displays cable interface information.
debug cable error	Displays errors that occur in the cable MAC protocols. To disable debugging output, use the no form of the command.
debug cable phs	Displays the activities of the PHS and restoration driver. The no form of this command disables debugging output.

Setting Optional Broadcast and Cable IP Multicast Echo

This configuration is optional. You can set additional IP parameters to enable downstream echoing of upstream data. This section contains two procedures to configure these optional IP parameters:

Note The default values for the commands used in these configuration steps are adequate in most cases to configure the Cisco CMTS routers.

Setting IP Multicast Echo

The Cisco uBR10012 router echoes IP multicast packets by default. To activate IP multicast echo if it has been previously disabled, use the following command in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable ip-multicast-echo`	Enables IP multicast echo. This is the default.

To disable IP multicast echo, enter the **no cable ip-multicast-echo** command in cable interface configuration mode.

Verifying IP Multicast Echo

To determine whether IP multicast echo is activated or deactivated, enter the **more system:running-config** command, and look for the cable interface configuration information. If IP multicast echo is activated, there is no notation in the output, because this is the default setting. If IP multicast echo is deactivated, a notation appears in the output:

```
Router# more system:running-config

Building configuration...

Current configuration:
!
interface cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 no cable ip-multicast-echo
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, make sure that you entered the correct slot and port numbers when you entered cable interface configuration mode.

Access Lists and the cable ip-multicast echo Command

The **cable ip-multicast-echo** command is enabled by default on the Cisco CMTS routers, so that multicast IP packets that arrive on the upstream at the Cisco CMTS are forwarded on the appropriate downstream ports so that they are delivered to the other CMs and CPE devices on that segment of the network. This allows the cable network to behave like a standard Ethernet network in terms of its handling of multicast IP traffic.

However, on the Cisco uBR10012 router, input access lists are not applied to the multicast traffic that is echoed on each downstream. To control the echoed multicast traffic, you therefore need to configure an output access list and apply it to each downstream interface.

Refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com for additional information on access lists and multicast echo:

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

Setting IP Broadcast Echo

By default, the Cisco uBR10012 router does not echo IP broadcast packets. To activate IP broadcast echo, use the following command in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable ip-broadcast-echo`	Enables IP broadcast echo.

To disable IP broadcast echo when it is enabled, enter the **no cable ip-broadcast-echo** command in cable interface configuration mode.

Verifying IP Broadcast Echo

To determine whether IP broadcast echo is activated or deactivated, enter the **more system:running-config** command and look for a notation in the cable interface configuration information:

```
Router# more system:running-config

Building configuration...

Current configuration:
!
interface cable5/0/0

ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable ip-broadcast-echo
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Cable Interface Configuration Examples

This section provides the following configuration examples:

Example: Subinterface Configuration

The following example shows how to define a subinterface on the cable5/0/0:

```
interface cable5/0/0
! No IP address
! MAC level configuration only

! first subinterface
interface cable5/0/0.1
description Management Subinterface
ip address 10.255.1.1 255.255.255.0
cable helper-address 10.151.129.2

! second subinterface
interface cable5/0/0.2
ip address 10.279.4.2 255.255.255.0
cable helper-address 10.151.129.2
```

```
! third subinterface
interface cable5/0/0.3
ip address 10.254.5.2 255.255.255.0
cable helper-address 10.151.129.2
```

Example: Cable Interface Bundling

The following example shows how to bundle a group of physical interfaces. In this example, the interfaces int c5/0/0 and int c4/0 are bundled.

```
int c5/0/0
ip address 209.165.200.225 255.255.255.0
ip address 209.165.201.1 255.255.255.0 secondary
cable helper-address 10.5.1.5
! MAC level configuration
cable bundle 1 master
int c4/0/0
! No IP address
! MAC layer configuration only
cable bundle 1
```

Example: Subinterface Definition on Bundle Master

The following example shows how to define subinterfaces on a bundle master and define Layer 3 configurations for each subinterface. In this example, the interfaces int c5/0/0 and int c4/0/0 are bundled.

```
int c5/0/0
! No IP address
! MAC level configuration only
cable bundle 1 master

int c4/0/0
! No IP address
! MAC layer configuration
cable bundle 1

! first subinterface
int c5/0/0.1
ip address 10.22.64.0 255.255.255.0
cable helper-address 10.4.1.2

! second subinterface
int c5/0/0.2
ip address 10.12.39.0 255.255.255.0
cable helper-address 10.4.1.2

! third subinterface
int c5/0/0.3
ip address 10.96.3.0 255.255.255.0
cable helper-address 10.4.1.2
```

Example: Cable Interface Bundle Master Configuration

The following example shows how to configure cable interface bundles:

```
Displaying the contents of the bundle
Router(config-if)# cable bundle ?
  <1-255>  Bundle number
Router(config-if)# cable bundle 25 ?
  master  Bundle master
  <cr>
Router(config-if)# cable bundle 25 master ?
  <cr>
Router(config-if)# cable bundle 25 master
```

```
Router(config-if)#
07:28:17: %uBR10000-5-UPDOWN: Interface Cable5/0/0 Port U0, changed state to down
07:28:18: %uBR10000-5-UPDOWN: Interface Cable5/0/0 Port U0, changed state to up
```

Example: PE Router Configuration

This example (system information display) identifies the version of Cisco IOS software installed and displays PE configurations:

```
! Defines the hostname of the Cisco uBR10012
hostname region-1-ubr
!
! Describes where the system is getting the software image it is running. In
! this configuration example, the system is loading a Cisco uBR10012 image named
! AdamSpecial from slot 0.
boot system flash slot0:uBR10000-p-mz.AdamSpecial
!
! Creates the enable secret password.
enable secret xxxx
enable password xxxx
!
! Sets QoS per modem for the cable plant.
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
! Allows the system to use a full range of IP addresses, including subnet zero, for
! interface addresses and routing updates.
ip subnet-zero
!
! Enables Cisco Express Forwarding.
ip cef
!
! Configures a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to insert the
! DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information option
!
! Enters the virtual routing forwarding (VRF) configuration mode and maps a VRF table to
! the virtual private network (VPN) called MGMT-VPN. The VRF table contains the set of
! routes that points to or gives routes to the CNR device, which provisions the cable
! modem devices. Each VRF table defines a path through the MPLS cloud.
ip vrf MGMT-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:1
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target export 100:2
 route-target export 100:3
!
! Maps a VRF table to the VPN called ISP1-VPN.
ip vrf ISP1-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:2
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target import 100:1
!
! Maps a VRF table to the VPN called ISP2-VPN.
ip vrf ISP2-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:3
!
! Creates a list of import and/or export route target communities for the VPN.
```

```
 route-target import 100:1
!
! Maps a VRF table to the VPN called MSO-isp. Note: MSO-isp could be considered ISP-3; in
! this case, the MSO is competing with other ISPs for other ISP services.
ip vrf MSO-isp
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:4
!
! Creates a list of import and/or export route target communities for the VPN.
  route-target import 100:1
!
! Builds a loopback interface to be used with MPLS and BGP; creating a loopback interface
! eliminates unnecessary updates (caused by physical interfaces going up and down) from
! flooding the network.
interface Loopback0
 ip address 10.0.0.0 255.255.255.0
 no ip directed-broadcast
!
! Assigns an IP address to this Fast Ethernet interface. MPLS tag-switching must be
! enabled on this interface.
interface FastEthernet0/0/0
 description Connection to MSO core.
 ip address 10.0.0.0 255.255.255.0
 no ip directed-broadcast
 full-duplex
 tag-switching ip
!
! Enters cable interface configuration mode and configures the physical aspects of the
! 5/0/0 cable interface. Please note that no IP addresses are assigned to this interface;
! they will be assigned instead to the logical subinterfaces. All other commands for
! this cable interface should be configured to meet the specific needs of your cable RF
! plant and cable network.
interface Cable5/0/0
 no ip address
 ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 855000000
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
!
! Configures the physical aspects of the 5/0/0.1 cable subinterface. If cable modems have
! not been assigned IP addresses, they will automatically come on-line using the settings
! for subinterface X.1.
interface Cable5/0/0.1
 description Cable Administration Network
!
! Associates this interface with the VRF and MPLS VPNs that connect to the MSO cable
! network registrar (CNR). The CNR provides cable modems with IP addresses and other
! initialization parameters.
 ip vrf forwarding MSO
!
! Defines a range of IP addresses and masks to be assigned to cable modems not yet associated
 with an ISP.
 ip address 10.0.0.0 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
```

```
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PCs that are not yet associated with an ISP.
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures the physical aspects of the 5/0/0.2 cable subinterface.
interface Cable5/0/0.2
 description MSO as ISP Network
!
! Assigns this subinterface to the MPLS VPN used by the MSO to supply service to
! customers——in this case, MSO-isp.
 ip vrf forwarding MSO-isp
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.0.0 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.1.0.0 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures the physical aspects of the 5/0.3 cable subinterface
interface Cable5/0/0.3
 description ISP1's Network
!
! Makes this subinterface a member of the MPLS VPN.
 ip vrf forwarding isp1
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Configures the physical aspects of the 5/0/0.4 cable subinterface
interface Cable5/0/0.4
```

```
 description ISP2's Network
!
! Makes this subinterface a member of the MPLS VPN.
 ip vrf forwarding isp2
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.2.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
!
 cable dhcp-giaddr policy
!
!! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
!
end
```

Example: Router Configuration

This example (system information display) identifies the version of Cisco IOS software installed and displays PE configurations:

```
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R7460-7206-02
!
enable password xxxx
!
ip subnet-zero
ip cef
ip host brios 223.255.254.253
!
interface Loopback0
 ip address 10.2.1.3 255.255.255.0
 no ip directed-broadcast
!
interface Loopback1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
!
interface FastEthernet0/0/0
 ip address 1.7.108.2 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
```

```
 full-duplex
 no cdp enable
!
router ospf 222
 network 10.0.1.0 255.255.255.0 area 0
 network 10.0.2.0 255.255.255.0 area 0
 network 10.0.3.0 255.255.255.0 area 0
 network 10.0.4.0 255.255.255.0 area 0
 network 20.2.1.3 255.255.255.0 area 0
!
ip classless
no ip http server
!
!
map-list test-b
no cdp run
!
tftp-server slot0:master/120/ubr10k-p6-mz.122-2.XF
!
line con 0
 exec-timeout 0 0
 password xxxx
 login
 transport input none
line aux 0
line vty 0 4
 password xxxx
 login
!
no scheduler max-task-time
end
```

Example: Configuring BGP Routing Sessions

To configure BGP routing sessions in a provider network, use the following commands in router configuration mode on the PE router:

Step 1 Configure the BGP routing process with the autonomous system number:

Example:

```
Router(config)# router bgp 42
```

Step 2 Specify a neighbor's IP address or BGP peer group, identifying it to the local autonomous system:

Example:

```
Router(config-router)# neighbor 200.28.28.40
Activate the advertisement of the IPv4address family.
Router(config-router)# neighbor 200.28.28.40 activate
```

Example: Configuring PE-to-PE Routing Sessions

To configure PE-to-PE routing sessions in a provider network, use the following commands in router configuration mode on the PE router:

Step 1 Define internal Border Gateway Protocol (iBGP) parameters for VPNv4 network-layer reachability information (NLRI) exchange:

Example:
```
Router(config-router)# address-family vpnv4 unicast
```

Step 2 Define an IBGP session to exchange VPNv4 NLRIs:

Example:
```
Router(config-router-af)# neighbor 200.28.28.45 remote-as 48
Router(config-router-af)# exit
```

Step 3 Activate the advertisement of the IPv4address family:

Example:
```
Router(config-router)# neighbor 200.28.28.45 activate
```

Example: Configuring BGP PE-to-CE Routing Sessions

To configure BGP PE-to-CE routing sessions, use the following commands in router configuration mode on the PE router:

Step 1 Define external Border Gateway Protocol (eBGP) parameters for PE-to-CE routing sessions:

Example:
```
Router(config-router)# address-family ipv4 unicast vrf
go_fast_internet_company
```

Step 2 Define an eBGP session between PE and CE routers and activate the advertisement of the IPv4 address family:

Example:
```
Router(config-router-af)# neighbor 200.28.28.46 remote-as 49
Router(config-router-af)# neighbor 200.28.28.46 activate
```

Example: Configuring RIP PE-to-CE Routing Sessions

To configure RIP PE-to-CE routing sessions, use the following commands in router configuration mode on the PE router:

Enable RIP, define RIP parameters for PE-to-CE routing sessions, and enable RIP on the PE-to-CE link:

Example:

```
Router(config)# router rip
Router(config-router)# address-family ipv4 unicast vrf
go_fast_internet_company
Router(config-router-af)# network 200.28.28.47
```

Example: Configuring Static Route PE-to-CE Routing Sessions

To configure static route PE-to-CE routing sessions, use the following commands in router configuration mode on the PE router:

Step 1 Define static route parameters for each PE-to-CE session and for each BGP PE-to-CE routing session.

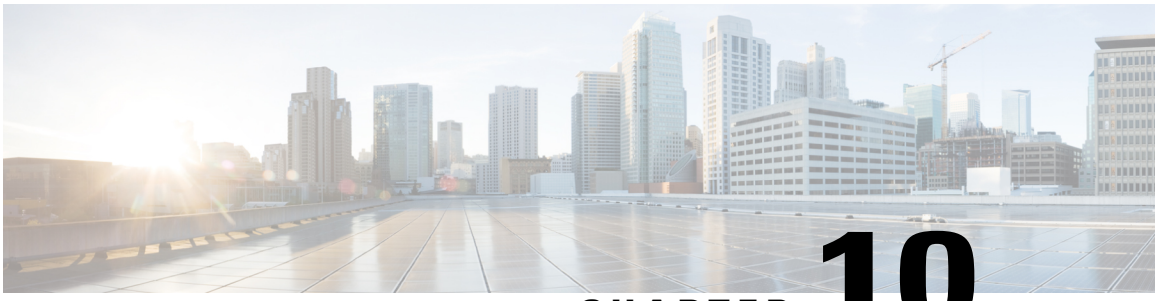
Example:

```
Router(config)# ip route vrf go_fast_internet_company 200.28.28.46
255.255.255.0 200.28.28.50
Router(config-router)# address-family ipv4 unicast vrf
go_fast_internet_company
```

Step 2 Redistribute VRF static routes and directly connected networks into the VRF BGP table.

Example:

```
Router(config-router-af)# redistribute static
Router(config-router-af)# redistribute static connected
```



CHAPTER 10

Configuring Upstream Cable Interface Features on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: June 19, 2013

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The cable interface in the Cisco universal broadband router supports downstream and upstream signals, and serves as the cable TV radio frequency (RF) interface. The downstream signal is output as an intermediate-frequency (IF) signal suitable for use with an external upconverter. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determines the combination of cable interfaces, network uplink line cards, and other components that you should use.

The Cisco IOS software command-line interface (CLI) can be used to configure the Cisco cable interface line card for correct operation on the hybrid fiber-coaxial (HFC) cable network. This chapter provides a configuration summary for the various upstream cable interface features available on a Cisco CMTS router. Details about some of these features can be found in other chapters of this book.

Note The configuration commands and examples in this chapter may show slot numbering or references to either Cisco uBR7200 series or Cisco uBR10012 Universal Broadband Routers. However, the features can be configured on either platform. Use the slot numbering appropriate for your CMTS router configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring Upstream Cable Interfaces on the Cisco CMTS Routers

The configuration of upstream cable interface features is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and Cisco IOS Release 12.2SC. The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 10: Configuring Upstream Cable Interfaces on the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE2 Cisco IOS Release 12.2(33)SCC • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [11]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[12]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

11 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

12 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Prioritizing Upstream Traffic to Initialize Cable Modems

When the Cisco CMTS is busy servicing data and bandwidth requests from a large number of online cable modems, it may deny new registration requests from offline cable modems. This denial of service occurs

because when a cable modem first begins initializing, its default upstream service flow is assigned a quality of service (QoS) profile-2 with a priority of zero. Zero is the lowest priority that can be scheduled. Depending on the priority and rate of bandwidth requests from other online cable modems, the priority-zero queue can either overflow or get ignored.

To ensure that the initializing cable modems can get online when a large number of online cable modems are actively transmitting data, the Cisco CMTS must allow the bandwidth request from an initializing cable modem to get priority over those requests from online cable modems.

In Cisco IOS Release 12.2(33)SCD2 and later releases, an operator can configure the priority of QoS profile-2 to a higher value.

Configuring the Priority of the QoS Profile

This configuration is optional. This section describes how you can manually configure a non-zero value for the QoS profile-2 priority to ensure that initialization requests from offline cable modems are serviced.

Note It is up to the cable operator to determine the appropriate new priority value.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos pre-registration us-priority** *priority-value* **Example:** `Router(config)# cable qos pre-registration us-priority 2`	Sets the priority of the QoS profile-2 of the initializing cable modem. **Note** The valid priority value range is 0 to 7 where 0 is the default value. • **us-priority—**Specifies the upstream priority to be assigned to the pre-registration traffic. • *priority-value***—**User-defined priority value for the QoS profile-2.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

After a cable modem has successfully completed registration, the QoS profile of the default upstream service flow is changed from QoS profile-2 to the QoS indicated through the DOCSIS configuration file.

What to Do Next

To determine if the priority of the QoS profile-2 is configured, enter the **show cable qos profile** command in privileged EXEC mode.

```
Router# show cable qos profile

ID  Prio Max       Guarantee Max        Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream tx    AND  OR    by      priv  rate
         bandwidth bandwidth bandwidth  burst mask mask          enab  enab
1   0    0         0         0          0     0xFF 0x0   cmts(r) no    no
2   2    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
Router#
```

The **Prio** column in the **ID 2** displays the user-defined value of the QoS profile-2.

Activating the Upstream Minimum Reserved Traffic Rate Plus Excess Traffic Rate

This configuration is optional. Each service flow (SF) carries traffic based on certain defined parameters. One of them is the minimum reserved traffic rate.

The minimum reserved traffic rate specifies the minimum traffic rate, in bits/sec, reserved for a service flow. The value of minimum reserved traffic rate is calculated from the byte following the MAC header check sequence (HCS) to the end of the cyclic redundancy check (CRC), including every protocol data unit (PDU) in a concatenated MAC frame. If this parameter is omitted, then it defaults to a value of 0 bits/sec (that is, no bandwidth is reserved for the flow by default).

The Cisco CMTS schedules forwarding traffic of all service flows such that each flow receives at least its minimum reserved traffic rate when transmitting packets with the assumed minimum reserved rate packet size. If the service flow requests less bandwidth than its minimum reserved traffic rate, the Cisco CMTS reallocates the excess reserved bandwidth for other purposes. All best effort service flows with or without their minimum reserved traffic rate configured, share the excess bandwidth.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable rate-limit-algorithm min-plus-excess** **Example:** `Router(config)# cable rate-limit-algorithm min-plus-excess`	Enables a service flow to receive its configured minimum reserved traffic rate plus the expected excess traffic rate bandwidth.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

What to Do Next

To verify if the upstream min-plus-excess parameter is configured and activated, run the **show interface cable mac-scheduler** and the **show interface cable service flow** commands in privileged EXEC mode.

```
Router# show interface cable 8/0/0 mac-scheduler 0 | include rate

DOCSIS 1.1 MAC scheduler for Cable8/0/0/U0: rate 10240000

Router# show interface cable 8/0/0 service-flow qos us

Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Through
          State       Type
7     US  act   1     BE     0    2000000     28000       500000      856051
134   US  act   120   BE     0    2000000     11000       0           403840
9     US  act   2     BE     0    2000000     28000       500000      856176
129   US  act   115   BE     0    2000000     11000       0           402647
11    US  act   3     BE     0    2000000     28000       500000      856019
132   US  act   118   BE     0    2000000     11000       0           402751
13    US  act   4     BE     0    2000000     28000       500000      856394
131   US  act   117   BE     0    2000000     11000       0           402754
15    US  act   5     BE     0    2000000     28000       500000      855977
135   US  act   121   BE     0    2000000     11000       0           403808
17    US  act   6     BE     0    2000000     28000       500000      685510
133   US  act   119   BE     0    2000000     11000       0           341456
25    US  act   13    BE     0    2000000     28000       500000      855598
130   US  act   116   BE     0    2000000     11000       0           403870
Router#
```

Activating Upstream Admission Control

Upstream admission control tallies up the total amount of guaranteed minimum upstream throughput reserved by CMs on an upstream interface. When the total exceeds an allowable level, no more CMs requiring a guaranteed minimum upstream rate are allowed online on that upstream port.

The Cisco CMTS upstream admission control is turned off by default and must be activated. To set the upstream admission control as a percentage of the upstream channel capacity, use the following command in cable interface configuration mode. The admission control is set as a percentage of the specified upstream channel capacity. The acceptable range is from 10 to 1000 percent.

```
Router(config-if)# cable upstream usport admission-control percentage
```

For example:

```
Router(config-if)# cable upstream 0 admission-control ?
    Max Reservation Limit As Percentage of Raw Channel Capacity
```

Note If *percentage* is left blank or set to 100%, the Cisco CMTS will only allow the total of the actual available upstream bandwidth to be guaranteed. If *percentage* is set to its maximum of 1000, then up to 10 times of the actual interface bandwidth may be "guaranteed".

Verifying Upstream Admission Control

To determine if upstream admission control is configured and activated, enter the **show running-config** command in privileged EXEC mode and look for the cable interface configuration information. If upstream admission control is configured and enabled, an admission control entry appears in the **show running-config** command output, indicating the user-defined percentage of upstream channel capacity allowable. If upstream admission control is disabled, no admission control entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

Activating Upstream Differential Encoding

Differential encoding on the upstream is a digital encoding technique whereby a binary value is denoted by a signal change rather than a particular signal level. To enable differential encoding on upstream traffic to a specified cable interface, use the following command in cable interface configuration mode. Upstream differential encoding is enabled by default.

```
Router(config-if)# cable upstream usport differential-encoding
```

Verifying Upstream Differential Encoding

To determine if upstream differential encoding is activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream differential encoding is enabled, a differential encoding entry appears in the **show running-config** output. If upstream differential encoding is disabled, no differential encoding entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.
Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.
Step 3 Ensure that the captive installation screws are tight.
Step 4 Verify that you have entered the correct slot and port numbers.
Step 5 Verify that you selected a valid frequency for your router.

Activating Upstream Forward Error Correction

The Cisco uBR7200 series CMTS uses forward error correction (FEC) to attempt to correct any upstream data that might have been corrupted. When FEC is activated, all CMs on the network also activate FEC.

Note Although upstream FEC is an option, it is recommended that you use upstream FEC. FEC is activated by default and should not be disabled.

To activate the upstream forward error correction and to enable FEC, use the following command in cable interface configuration mode.

```
Router(config-if)# cable upstream usport fec
```

Verifying Upstream FEC

To verify whether FEC is activated or deactivated, enter the **more system:running-config** command and look for the cable interface configuration information. If FEC is enabled, an FEC entry appears in the **show running-config** command output. If FEC is disabled, no FEC entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.
Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.
Step 3 Ensure that the captive installation screws are tight.
Step 4 Verify that you have entered the correct slot and port numbers.
Step 5 Verify that you selected a valid frequency for your router.

Activating the Upstream Ports

Each upstream port must be activated to enable upstream data transmission from the CMs on the HFC network to the Cisco uBR7200 series CMTS.

Note The upstream cable interface does not operate until you either set a fixed upstream frequency or create and configure a spectrum group. For more information, see the Setting the Upstream Frequency, on page 249.

To activate the upstream ports, perform the following steps:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/port* **Example:** `Router(config)# interface cable 5/0`	Specifies a cable interface and enters cable interface configuration mode.
Step 4	**no cable upstream** *usport* **shutdown** **Example:** `Router(config-if)# no cable upstream 0 shutdown`	Enables upstream data traffic.

What to Do Next

To determine if the upstream ports are activated or deactivated, enter the **show interface cable** command for the upstream port just configured:

```
Router# show interface cable5/0

Cable5/0 is up, line protocol is up
 Hardware is BCM3210 FPGA, address is 00e0.1e5f.7a60 (bia 00e0.1e5f.7a60)
 Internet address is 1.1.1.3/24
 MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
 Encapsulation, loopback not set, keepalive not set
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:25, output 00:00:00, output hang never
 Last clearing of "show interface" counters never
 Queuing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sea, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
     10878 packets input, 853740 bytes, 0 no buffer
     Received 3679 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5401 packets output, 645885 bytes, 0 underruns
     0 output errors, 0 collisions, 9 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Activating Upstream Power Adjustment

To enable upstream power adjustment for a specified cable interface, use one of the following commands in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable upstream power-adjust continue`*pwr-level*	Sets the minimum power adjustment in dB that allows continued ranging status. Valid values are 2 to 15 dB. Default = 4 dB.
`Router(config-if)# cable upstream usport power-adjust noise`perc-pwr-adj	Sets the minimum number (percentage) of power-adjustment packets required to justify changing the upstream power rating. Valid values are 10 to 100 percent. The default is 30 percent.
`Router(config-if)# cable upstream 0 power-adjust threshold`*value*	Sets the power-adjustment threshold in dB. Valid values are 0 to 2 dB. The default is 1 dB.
`Router(config-if)# end` `Router#`	Returns to enable (privileged EXEC) mode.

To return the automatic upstream power-adjustment ranging value to the default of 4 dB, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream n power-adjust continue
```

To return the automatic upstream power-adjustment noise value to the default of 30 percent, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream n power-adjust noise
```

To return the upstream power-adjustment threshold value to the default of 1 dB, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream n power-adjust threshold
```

What to Do Next

To determine if upstream power adjustment is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream power adjustment is enabled, any or all three of the continue, noise, and threshold power-adjustment entries appear in the **show running-config** command output. If all three upstream power adjustments are disabled, no power-adjustment entry appears in the **show running-config** command output.

Activating the Upstream Scrambler

The scrambler on the upstream RF carrier enables CMs on the HFC network to use built-in scrambler circuitry for upstream data transmissions. The scrambler circuitry improves reliability of the upstream receiver on the cable interface line card.

Caution The upstream scrambler is activated by default and should not be disabled under normal circumstances. Disabling it can result in corrupted packets. Disable it only for prototype modems that do not support the upstream scrambler.

To activate the upstream scrambler, use the following command in cable interface configuration mode. The upstream scrambler is enabled by default.

```
Router(config-if)# cable upstream usport scrambler
```

Verifying the Upstream Scrambler

To determine if the upstream scrambler is activated, enter the **more system:running-config** command and look for the cable interface configuration information. Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

Activating Upstream Timing Adjustment

To enable upstream timing adjustment for a specified cable interface, use one of the following commands in cable interface configuration mode.

Command	Purpose
`Router(config-if)# cable upstream usport time-adjust continue seconds`	Sets the minimum timing adjustment that allows continued ranging status. Valid second values are 2 to 64 seconds. The default is 2 seconds.
`Router(config-if)# cable upstream usport time-adjust threshold seconds`	Sets the timing adjustment threshold value in seconds. Valid second values are 1to 32 seconds. The default is 1 second.
`Router(config-if)# end` `Router#`	Returns to enable (privileged EXEC) mode.

To return the upstream time-adjustment ranging value to the default of 2 seconds, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport time-adjust continue
```

To return the upstream time adjustment threshold value to the default of 1 second, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport time-adjust threshold
```

Verifying Upstream Timing Adjustment

To determine if upstream timing adjustment is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream timing adjustment is enabled, either or both of the continue and threshold timing-adjustment entries appear in the **show running-config** command output. If both the continue and threshold upstream timing adjustments are disabled, no timing adjustment entry appears in the **show running-config** command output.

Perform the following steps if you are having difficulty with verification:

Step 1 Verify that the cable connections are not loose or disconnected.

Step 2 Verify that the cable interface line card is firmly seated in its chassis slot

Step 3 Verify that the captive installation screws are tight.

Step 4 Confirm that you have entered the correct slot and port numbers.

Traffic Shaping

Traffic shaping basically uses queues to limit data surges that can congest a network. The data is buffered and then sent into the network in regulated amounts to ensure that the traffic fits within the expected traffic envelope for the particular connection.

Traffic shaping reduces the chance of retransmitting information to hosts on the cable plant. When cable modems (CMs) have rate limits established, the CMTS typically drops bandwidth requests to enforce the rate limit. This causes the CM to retransmit the request, thereby putting additional latency in packet transmission. If both the hosts sending and requesting information are on the same cable plant, the upstream bandwidth is wasted as well.

On the DOCSIS downstream and upstream channels, traffic shaping allows the CMTS to perform downstream rate limiting and bandwidth request shaping allows the CMTS to perform upstream rate limiting. Rate limiting restricts the data rate to and from a CM; the MAC scheduler supports shaping capabilities for downstream and upstream traffic. Rate limiting ensures that no single CM consumes all of the channel bandwidth and allows a CMTS administrator to configure different maximum data rates for different subscribers. Subscribers requiring higher sustained rates and willing to pay for higher rates can be configured with higher sustained rate limits in their CM DOCSIS configuration file over regular subscribers, who pay less and get lower rate limits.

Each time a packet belonging to a flow is transmitted on an output channel, the token-bucket policer function checks the rate limit status of the flow, parsing the following parameters:

- Token bucket maximum sustained rate in bits per millisecond.
- Token bucket depth (maximum transmit burst) in bits.
- Length of current packet to be sent in bits.

- Pointer to the token bucket of the flow.
- Pointer to the flow's token bucket last update time stamp.
- Variable to return the milliseconds buffering delay in case the packet needs to be shaped.
- Maximum buffering delay that the subsequent traffic shaper can handle in milliseconds.

Every flow has its own shaping buffer where rate-exceeded packets are typically held back in first-in/first-out (FIFO) order for later releases transmission.

Tip Token bucket policing with shaping is the per-upstream default rate limiting setting at the CMTS. Shaping can be enabled or disabled for the token-bucket algorithm.

Upstream Traffic Shaping

Upstream traffic shaping allows the CMTS to perform rate limiting on a DOCSIS upstream channel. The upstream traffic shaping feature delays the scheduling of the upstream packet, which in turn, causes the packet to be buffered on the cable modem device. This allows the user TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined quality of service (QoS) levels. Upstream traffic shaping enables the CMTS to enforce the peak upstream rate for each CM without degrading overall TCP performance for the subscriber CMs.

When you do not enable the shaping option for upstream rate limiting, the CMTS upstream-rate-policing code drops bandwidth requests from cable modems 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.

Upstream grant shaping is on a per-CM (service identifier-SID) basis. The grant shaping feature is a configurable option for the current upstream token-bucket rate-limiting algorithm.

A traffic shaping feature is restricted QoS class assignment, which allows a CMTS administrator to override the class of service provisioned for a CM. When this feature is enabled, the user-defined QoS profile is enforced on the CM attempting to register with the CMTS, regardless of the CM's provisioned class of service. Use the **cable qos profile** command to configure a QoS profile.

Note The restricted QoS class assignment feature is added to address instances where a cable operator implemented rate limiting incorrectly. The feature allows an administrator to override the statically provisioned QoS parameters of the CM and force the CM to use a specific QoS profile defined at the CMTS.

Upstream Buffer Control for Maximum Queue Depth

Upstream traffic shaping uses queues to control the upstream data flow. The data packets are buffered in a queue on the CM to regulate traffic and avoid network congestion. Starting with Cisco IOS Release 12.2(33)SCF2, the Upstream Buffer Control feature enables the Cisco CMTS to control the size of this queue (or buffer) by controlling the amount of data that can be enqueued for transmission at any point of time.

The Upstream Buffer Control feature supports buffer control TLVs, which allows the user to configure the buffer size control parameters. These parameters are used to create buffer for each service flow on the CM. The buffer control parameters comprise of three values—minimum buffer, maximum buffer, and target buffer. The minimum buffer and maximum buffer parameters provide a range for the size of the service flow buffer, and the target buffer parameter indicates a desired size of the buffer. The Upstream Buffer Control feature supports the following sub-TLVs in the service flow TLV (24.35), to control these buffer parameters:

Table 11: Supported Upstream Buffer Control TLVs

TLV	TLV Description
24.35.1	Upstream minimum buffer.
24.35.2	Upstream target buffer
24.35.3	Upstream maximum buffer

The CM sends the buffer control TLVs in the registration request or in dynamic service add (or change) request to the Cisco CMTS. The Cisco CMTS stores the value of the buffer control TLVs and sends its response. On receiving the response CM creates a buffer for US service flow based on the TLVs.

The buffer control parameters can be configured in the CM configuration file, or by using the cable service class command in global configuration mode. For more information on how to configure upstream buffer control parameters, see Setting Upstream Buffer Control Parameters, on page 256.

Configuring Upstream Rate Limiting and Traffic Shaping

You can configure rate limiting and traffic shaping on a DOCSIS upstream channel. This delays the scheduling of the upstream packet, which in turn causes the packet to be buffered on the cable CPE device. This allows the user's TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined QoS levels.

To configure this, use the following command in cable interface configuration mode.

Command	Purpose
`Router(config-if)# [no] cable upstream <n1> rate-limit [token-bucket]`	Enables or disables DOCSIS rate limiting or shaping on an upstream channel. <n1> depends on the number of upstream channels on the specific cable interface line card.

Using Cisco IOS Release 12.0(5)T1 or higher, the software supports:

- Generic calendar queuing routines
- New token bucket policing function
- Grant shaping application of the calendar queues
- Upstream rate shaping option to the token-bucket keyword

- A default state change from 1 second burst policing to token-bucket with shaping

Tip Upstream grant shaping is per CM (SID). Shaping can be enabled or disabled for the token-bucket algorithm.

Note Before the introduction of this feature, the CMTS would drop bandwidth requests from a CM it detected as exceeding its configured peak upstream rate. Such request dropping affects the throughput performance of IP-based protocols such as FTP, TCP, and SMTP. With this feature, the CMTS can shape (buffer) the grants for a CM that is exceeding its upstream rate, rather than dropping the bandwidth requests.

```
Router# show interface cable 3/0 sid 1 counters

Sid   Inpackets  Inoctets   Outpackets Outoctets  Ratelimit  Ratelimit
                                                  BWReqDrop  DSPktDrop
1     67859      99158800   67570      98734862   2579       0
```

Setting Upstream Backoff Values

The DOCSIS-specified method of contention resolution for CMs wanting to transmit data or requests on the upstream channel is a truncated binary exponential backoff value, with the initial backoff window and the maximum backoff window controlled by the CMTS. The Cisco uBR7200 series CMTS specifies backoff window values for both data and initial ranging, and sends these values downstream as part of the Bandwidth Allocation Map (MAP) MAC message.

The values are configurable on the Cisco uBR7200 series software and are power-of-two values. For example, a value of 4 indicates a window between 0 and 15; a value of 10 indicates a window between 0 and 1023. You can set fixed start and end values for data backoff on the upstream ports, or you can set the upstream ports for automatic data backoff. You have the same options for ranging backoff. For both backoff windows, the default start value is 0; the default end value is 4. Valid values are from 0 to 15.

Note It is not recommended that you adjust default values, but that you enable the automatic dynamic backoff algorithm.

To set data or ranging backoff values for an upstream port, use one or more of the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enter one of the following commands: • Router(config-if)#**cable upstream** *usport* **data-backoff** *start end* • Router(config-if)#**cable upstream** *usport* **data-backoff automatic**	Optimizes the **automatic** setting for as many as 250 cable interfaces per upstream port. Sets manual values for data backoff windows only when operating with more than 250 cable interfaces per upstream port. Configures the default backoff window values of 0 and 4.

	Command or Action	Purpose
Step 2	Enter one of the following commands: • Router(config-if)#**cable upstream** *usport* **range** *start end* • Router(config-if)#**cable upstream** *usport* **range automatic**	Optimizes the **automatic** setting for as many as 250 cable interfaces per upstream port. Sets manual values for data backoff windows only when operating with more than 250 cable interfaces per upstream port. Configures the default backoff window values of 0 and 4.

When considering whether to adjust backoff values, keep the following considerations in mind:

- The cable interface reconnection time after a power outage is related to the following factors:
  - DHCP, ToD, and TFTP servers often operate well below 1 percent load under normal situations, but can jump to over 100 percent after an outage.
  - Adjusting the backoffs to larger numbers slows cable interface reconnection and reduces server load.
  - Backoffs that are too small result in cable interfaces failing to range the upstream RF levels correctly and cycling to maximum power, thus increasing connection time and reducing network performance.
  - Backoffs that are too large result in increased recovery time after a large service outage.
  - There is significant variation in cable interface performance (brand to brand) in cable interface restart time.
- All cable interfaces should recover in 0 to 10 minutes after all services are restored (Cisco uBR7200 series, RF transport, DHCP, TFTP, and ToD servers). A CM that takes longer than 10 minutes could be experiencing a problem with the modem itself, a problem with CMTS settings, or a problem in the DOCSIS provisioning servers.

Note Upstream segments serving a relatively large number of cable interfaces (for example, more than 1600) might suffer recovery times greater than 10 minutes.

What to Do Next

To verify backoff window settings, enter the **show controllers cable** command for the upstream port you configured:

```
Router# show controllers cable5/0 upstream 0

Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
  part_id=0x3137, rev_id=0x03, rev2_id=0xFF
```

```
nb_agc_thr=0x0000, nb_agc_nom=0x0000
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 8
Minislot Size in Symbols = 64
Bandwidth Requests = 0xFE
Piggyback Requests = 0xD
Invalid BW Requests= 0x2
Minislots Requested= 0x2963
Minislots Granted  = 0x2963
Minislot Size in Bytes = 16
Map Advance = 4000 usecs
UCD Count = 32964
DES Ctrl Reg#0 = C000C043, Reg#1 = 0
```

Setting the Upstream Channel Width

Use the commands below to enter the upstream channel width in hertz (Hz). For NTSC operations, valid values are 200000 Hz (160 kilo symbols per second [ksps]), 400,000 Hz (320 ksps), 800,000 Hz (640 ksps), 1,600,000 Hz (1280 ksps), and 3,200,000 Hz (2560 ksps). The default is 1,600,000 Hz.

If no acceptable channels of the specified width are found, the spectrum management card automatically begins to scan the upstream spectrum for the next largest available channel width; for example, if the spectrum management card is unable to find a usable 1.6 MHz upstream channel, it automatically begins searching for usable 800 kHz channels.

Caution Higher symbol rates are more susceptible to RF noise and interference. If you use a symbol rate or modulation format beyond the capabilities of your HFC network, you might experience packet loss or loss of cable interface connectivity.

Note For QAM-16 channel widths of 400 kHz (320 ksps) or greater, Cisco recommends that you use QAM-16 modulation for long and short data, and that you use QPSK for request, initial, and station communications. For QAM-16 channel widths of 200 kHz (160 ksps), all communication must be able to use QAM-16. That is, 160 ksps with QAM-16 requires an exceptional signal-to-noise ratio (SNR) in your upstream channels. When you use QAM-16 for request, initial, and station maintenance messages with channel widths greater than 400 kHz, the QAM-16 preamble and message data take longer to transmit than the QPSK format.

To set the upstream channel width, use the following commands in cable interface configuration mode:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)#**cable upstream** *usport* **channel-width** *width*	Enters the channel width for your upstream RF carrier in Hz.
Step 2	Router(config-if)#**no cable upstream** *usport* **channel-width**	Returns the channel width to its default setting of 1,600,000 Hz.

For additional information about channel width and minislot size, refer to the Cable Radio Frequency (RF) FAQs on Cisco.com.

Verifying Upstream Channel Width

To verify the current value of the upstream channel width, enter the **show controllers cable** command for the upstream port you configured:

```
Router# show controllers cable5/0 upstream 0

Cable5/0 Upstream 0 is up
  Frequency 24.016 MHz, Channel Width 0.800 MHz, QPSK Symbol Rate 0.640 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
```

Perform these steps if you are having difficulty with verification:

Step 1 Use a valid combination of modulation format (QPSK and QAM-16), minislot size, frequency, and the **no shutdown** command.

Step 2 Use a recommended or previously tested modulation profile. It is not uncommon to create a modulation profile that does not allow cable interface-to-headend communication. Because each message type is individually specified, some messages might not work.

Step 3 Verify using IP ping packets of varying lengths (64 to 1500 bytes). Ping from the headend to the cable interface.

Step 4 Verify with your cable interface vendor that your CM software is fully certified or compatible with DOCSIS 1.0 and extensions, as appropriate.

Copy and Paste Support for TDMA to A-TDMA Upgrade

When configuration is copied from Method of Procedure (MOP) document and pasted, with 6400 kHz specified as channel width (as last-choice-width or first-choice-width or both) and the DOCSIS mode set to TDMA or mixed TDMA/A-TDMA mode, the 6400 kHz channel width is rejected. If the configuration is pasted twice, the 6400 kHz channel width is accepted.

To have the 6400 kHz accepted by pasting the configuration only once, Cisco IOS Release 12.2(33)SCG2 introduces the Copy and Paste Support for TDMA to A-TDMA Upgrade feature. If 6400 kHz is set as channel width in TDMA mode or mixed TDMA/A-TDMA mode, DOCSIS mode automatically changes to A-TDMA-only (DOCSIS 2.0) mode. The command interface displays a message to show the change in the DOCSIS mode.

The automatic change to the DOCSIS mode applies to logical upstream chanels configured for a physical

Note Only A-TDMA and SCDMA modes support 6400 kHz channel width. To configure 6400 kHz channel width with SCDMA mode, use manual configuration. The 6400 kHz channel width is hidden in CLI Interactive Help output for TDMA and mixed TDMA/A-TDMA modes.

Setting the Upstream Frequency

The upstream channel frequency of your RF output must be set to comply with the expected input frequency of your Cisco cable interface line card. To configure upstream channel frequencies, perform one of the following tasks:

- Configure a fixed frequency from 5 to 42 MHz for NTSC operations, then enable the upstream port.
- Create a global spectrum group, assign the interface to it, and enable the upstream port.

Note You can also select a default that does not set a specific fixed value.

Note The upstream port is frequency agile. If you define spectrum groups, the frequency can change while the interface is up and carrying traffic.

A modulation profile consists of a table of physical layer characteristics for the different types of upstream bursts; for example, initial maintenance, long grant, request/data, request, short grant, and station maintenance.

Note The upstream cable interface does not operate until you either set a fixed upstream frequency or create and configure a spectrum group. If you are setting a fixed upstream frequency, make sure that the frequency selected does not interfere with the frequencies used for any other upstream applications running on the cable plant.

To set a fixed upstream frequency, use the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **cable upstream** *usport* **frequency** *up-freq-hz*	Enters the fixed center frequency for your upstream RF carrier in Hz.
Step 2	Router(config-if)# **no cable upstream** *usport* **shutdown**	Places the upstream port in the “admin up” state.

Tip For National Television Standards Committee (NTSC) operations, valid ranges are 5000000 to 42000000 Hz.

Caution Some cable systems cannot reliably transport frequencies near these band edges. The wider the upstream channel (in MHz), the more difficulty you might have. Enter a center frequency between 20 and 38 MHz if you have difficulty.

Note You can also select a default that does not set a specific fixed value. The Cisco uBR7200 series software instructs the cable interfaces to use this frequency as the center frequency.

Note After the spectrum-band is changed, the spectrum management does not rearrange the frequency for each US channel if the previous frequency belongs to the range of new spectrum-band, which means that the US frequency will not be changed; if the previous frequceny is out of range of new spectrum-band, those US channels will not get frequencies.

Verifying the Upstream Frequency

To verify the current value of the upstream frequency, enter the **show controllers cable** command for the upstream port you configured:

```
Router# show controllers cable5/0 upstream 0

Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
```

Note The upstream frequency displayed in the **show controllers cable** command output might not match the frequency that you entered when you set the upstream frequency. The Cisco uBR7200 series CMTS might select an upstream frequency close to the frequency you entered that offers better performance. The Cisco uBR7200 series CMTS selects the closest frequency available.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you have selected a valid frequency for your router.

Setting the Upstream Input Power Level

The Cisco uBR7200 series CMTS controls the output power levels of CMs to meet the desired upstream input power level. The nominal input power level for the upstream RF carrier is specified in decibels per millivolt (dBmV). The default setting of 0 dBmV is the optimal setting for the upstream power level.

The valid range for the input power level depends on the data rate. At 1.6 MHz, the valid range is –10 to 25 dBmV. If your power levels operate at greater than the maximum valid level, use an inline attenuator to bring the power level to within the valid range.

Caution If you increase the input power level, CMs on your HFC network increase their transmit power level. This increases the carrier-to-noise ratio (C/N) on the network, but also increases distortion products. Composite Second Order Beat (CSO) and Composite Triple Beat (CTB) values worsen by 2 dB for every 1 dB-increased C/N. The return path laser immediately enters a nonlinear mode called clipping, and all communication becomes unreliable. Many return lasers send short bursts above the clipping thresholds and fail on longer or successive bursts.

You should not adjust your input power level by more than 5 dB in a 30-second interval. If you increase the power level by more than 5 dB within 30 seconds, cable interface service on your network is disrupted. If you decrease the power level by more than 5 dB within 30 seconds, cable interfaces on your network are forced offline.

Note When you run the **cable upstream 0 power-level** command, Cisco recommends that the adjacent channel not have a large variation. The recommended maximum input power variance is 5 to 6 dBmV.

To set the upstream input power level in dBmV, use the following command in cable interface configuration mode. The default is 0 dBmV.

```
Router(config-if)# cable upstream usport power-level dbmv
```

Verifying the Upstream Input Power Level

To verify the current value of the upstream input power level, enter the **show controllers cable** command for the upstream port you configured:

```
Router# show controllers cable5/0 upstream 0

Cable5/0 Upstream 0 is up
  Frequency 24.016 MHz, Channel Width 0.800 MHz, QPSK Symbol Rate 0.640 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
```

Perform these steps if you are having difficulty with verification:

Step 1 Verify that the upstream amplitude of an optimal RF carrier (injected at the fiber node reference input point) reaches the cable interface line card input point at a consistent level (node-to-node and port-to-port).

Step 2 Verify that this absolute level, as installed, matches both the design and software settings on the Cisco uBR7200 series CMTS.

Note Software adjustments of 1 to 3 dB can be used to adjust for minor variations in measurement or setup and port-to-port calibration differences. These adjustments can significantly improve cable interface performance, especially in marginal situations. Larger adjustments should be made in conjunction with spectrum analyzer support at the headend or distribution hub.

Specifying Upstream Minislot Size

To specify the minislot size (in ticks) for specific upstream cable interfaces, use the following command in cable interface configuration mode. Acceptable values are 2, 4, 8, 16, 32, 64, and 128. The default is 8.

```
Router(config-if)# cable upstream usport minislot-size  size
```

For additional information about channel width and minislot size, refer to the Cable Radio Frequency (RF) FAQs on Cisco.com.

Verifying Upstream Minislot Size

To verify upstream minislot size, enter the **show controllers cable** command for the upstream port you configured:

```
Router# show controllers cable5/0 upstream 0

Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
  part_id=0xFFFF, rev_id=0xFF, rev2_id=0xFF
  nb_agc_thr=0x0000, nb_agc_nom=0x0000
  Range Load Reg Size=0x58
  Request Load Reg Size=0x0E
  Minislot Size in number of Timebase Ticks is = 8
  Minislot Size in Symbols = 64
  Bandwidth Requests = 0xFE
  Piggyback Requests = 0xD
  Invalid BW Requests= 0x2
  Minislots Requested= 0x2963
  Minislots Granted  = 0x2963
  Minislot Size in Bytes = 16
  Map Advance = 4000 usecs
  UCD Count = 32964
```

```
DES Ctrl Reg#0 = C000C043, Reg#1 = 0
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

Setting Upstream Traffic Shaping

Upstream traffic shaping, available on the DOCSIS upstream channel, delays the scheduling of the upstream packet, which in turn causes the packet to be buffered on the cable customer premises equipment (CPE) device. This allows the user's TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined quality of service (QoS) levels.

The bandwidth requests are buffered without incurring DOCSIS-related timeouts and retransmits. This enables the CMTS to enforce the peak upstream rate for each CM, without degrading overall TCP performance for the subscriber CPEs. Upstream grant shaping is per cable interface (per service ID (SID)).

Token-bucket policing with shaping is the per-upstream default rate-limiting setting at the CMTS. Shaping can be enabled or disabled for the token-bucket algorithm.

To enable upstream shaping for an upstream port on a Cisco cable interface line card, use one of the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enter the following commands: **Example:** `Router(config-if)# cable upstream usport rate-limit` `Router(config-if)# cable upstream usport rate-limit token-bucket` `Router(config-if)# cable upstream usport rate-limit token-bucket shaping`	Enables traffic shaping for the specified upstream cable interface. Enables traffic shaping for the upstream cable interface employing the token-bucket policing algorithm. Enables traffic shaping for the upstream cable interface employing the token-bucket policing algorithm with traffic shaping.
Step 2	**end** **Example:** `Router(config-if)# end`	Exits back to the EXEC mode so that you can verify upstream traffic shaping.

To disable upstream traffic shaping for an upstream port, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport rate-limit
```

The software supports:

- Generic calendar queuing routines
- New token-bucket policing function
- Grant shaping application of the calendar queues
- Upstream rate-shaping option to the token-bucket keyword
- A default state change from 1-second burst policing to token bucket with shaping

Tip Upstream grant shaping is per CM (per service ID (SID)). Shaping can be enabled or disabled for the token-bucket algorithm.

Note Before the introduction of this feature, the CMTS would drop bandwidth requests from a CM it detected as exceeding its configured peak upstream rate. Such request dropping affects the throughput performance of IP-based protocols such as FTP, TCP, and Simple Network Management Protocol (SNMP). With this feature, the CMTS can shape (buffer) the grants for a CM that is exceeding its upstream rate, rather than dropping the bandwidth requests.

```
Router# show interface cable 5/0 sid 1 counters

00:02:23: %ENVM-3-LASTENV: Cannot save environmental data
Sid  Req-polls  BW-reqs    Grants     Packets    Frag       Concatpkts
     issued     received   issued     received   complete   received
1    0          22         22         22         0          0
2    0          3          3          2          0          0
3    0          0          0          0          0          0
```

Verifying Upstream Bandwidth Request Shaping

To determine if upstream bandwidth request shaping is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream bandwidth request shaping is configured and enabled, a shaping entry appears in the **show running-config** output. If upstream bandwidth request shaping is disabled, **no cable upstream rate-limit** appears in the output.

You can also perform the following tasks to verify that bandwidth request shaping is enabled on the upstream channel:

Step 1 Configure a low-peak upstream rate limit for the CM in its QoS profile. Either use the CLI to modify the QoS profile of the modem, or edit the TFTP configuration file of the modem. For more information, see the DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers feature.

Step 2 Use a regular rate-limiting algorithm on the upstream without rate shaping, and note the drops of the excess bandwidth requests from this CM when it exceeds its peak upstream rate.

Use the **show interface cx/y sid counters verbose** command to see the bandwidth request drops. Verify that the upstream rate received by that modem is less than its configured peak rate, due to the timeouts and backoffs produced by the drop in bandwidth requests. Enter the **show interface cx/y service flow qos** command to see the input rate at CMTS in bps.

Step 3 Enable grant shaping on the upstream channel by using the new **shaping** keyword extension to the token-bucket algorithm CLI command.

Step 4 Make the CM exceed its peak upstream rate by generating upstream traffic, and note the effect of grant buffering (shaping) at the CMTS. If you use CM-to-CMTS pings, there is a perceivable decrease in the frequency of the pings.

Let the pings run long enough to allow the averages at the CMTS to settle; then view the upstream rate received by this single modem. Use the **show interface cx/y** command and see the input rate in bps. This value should be close to the modem's peak upstream rate. Also note the drop counts for the modem's SID by using the **show interface sid counters** command, and verify that the CMTS no longer drops the bandwidth requests from the CM.

The bandwidth request drop count (from the previous nonshaping test) remains unchanged when upstream rate shaping is used, indicating that the CMTS is actually shaping (buffering) the grants for the modem. Verify that the input rate at the CMTS (from the single rate-exceeded CM) stabilizes close to the configured peak rate of 128 Kbps.

Troubleshooting Tips

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

Configuring Upstream Drop Classifier

This configuration in optional. A set of matching criteria is applied by the cable modems to packets to determine if a packet should be dropped. This set of matching criteria when applied to upstream traffic, is called the Upstream Drop Classifier (UDC).

The CMTS enables the UDC feature on the cable modems. The UDC configuration is done by the cable modem using a configuration file.

Effective with Cisco IOS Release 12.2(33)SCG5, the UDC feature can be enabled for all cable modems on any interface of a Cisco CMTS by using the **cable udc-capability** command in interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router(config)# interface cable 7/1/0`	Enters the interface configuration mode
Step 4	**cable udc-capability** **Example:** `Router(config-if)# cable udc-capability`	Enables the UDC feature on cable modems.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

To verify that the UDC feature is enabled on a specified cable modem, use the **show cable modem** *H.H.H* **verbose** command (where *H.H.H* represents the MAC address of the cable modem) in privilege EXEC mode. The following example displays the output of the show command using the '|' and **section** keyword to show only the "UDC Enabled" field.

```
Router# show cable modem 4458.2945.3004 verbose | s UDC

UDC Enabled                     : Y

Router#
```

If the UDC feature is not enabled, this field shows 'N' to denote that the cable modems have not configured UDC.

Setting Upstream Buffer Control Parameters

This configuration is optional. To configure the upstream buffer control parameters for the CM queue using the service class name, use the cable service class command in global configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service class** *class-index* **max-buff-size** | **min-buff-size** | **tar-buff-size** **Example:** `Router(config)# cable service class 10 min-buff-size 1000`	Configures the following buffer control parameters. • *class-index*—The class ID for the class to be modified. • **max-buff-size—**Maximum CM buffer size. • **min-buff-size—**Minimum CM buffer size. • **tar-buff-size—**Target CM buffer size.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Upstream Buffer Control Parameters

To verify the current values of the upstream buffer control parameters for a particular service class, use the **show cable service-class verbose** command in privilege EXEC mode. The following is a sample output of the **show cable service-class verbose** command for a service class with class-index 10:

```
Router# show cable service-class 10 verbose

Index:                                  10
Name:                                   REG-US
Direction:                              Upstream
Traffic Priority:                       0
Maximum Sustained Rate:                 0 bits/sec
Max Burst:                              3044 bytes
Minimum Reserved Rate:                  0 bits/sec
Minimum Packet Size                     0 bytes
Peak Rate                               0 bits/sec
Admitted QoS Timeout                    200 seconds
Active QoS Timeout                      0 seconds
Maximum Concatenated Burst:             1522 bytes
Scheduling Type:                        Best Effort
Request/Transmission Policy:            0x0
IP ToS Overwrite [AND-mask,OR-mask]:    0xFF,0x0
Parameter Presence Bitfield:            {0x8, 0x0}
!Upstream Buffer Control Parameters
Minimum Buffer Size:                    1000 bytes
Target Buffer Size:                     1500 bytes
Maximum Buffer Size:                    2000 bytes
```

To verify if the upstream buffer control parameters have been correctly propagated to the CM, use the **show cable modem service-flow verbose** command, in privilege EXEC mode. The following is a sample output of the **show cable modem service-flow verbose** command for a particular CM:

```
Router# show cable modem 0022.cea5.02ba service-flow verbose

SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num  Primary
DS
                               Interface     State         Sid   CPE  Downstrea   RfId
0022.cea5.02ba 5.60.122.132    C7/1/0/UB     w-online      10    0     In7/1/0:0  840
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughp
          State       Type
29    US  act   10    BE     0    100000      3044        0           0
30    DS  act   N/A   BE     0    200000      3044        0           0

CfrId  SFID     CM Mac Address  Direction  State    Priority  Matches
Reg Info Requests Tx        : 2
Reg Info TLV len            : 152

UPSTREAM SERVICE FLOW DETAIL:
Sfid                                  : 29
Mac Address                           : 0022.cea5.02ba
Type                                  : Primary
Direction                             : Upstream
Current State                         : Active
Current QoS Indexes [Prov, Adm, Act]  : [3, 4, 4]
Active Time                           : 03:45
Required Attributes                   : 0x00000000
Forbidden Attributes                  : 0x00000000
Aggregate Attributes                  : 0x00000000
Sid                                   : 10
Service Class Name                    : REG-US
Traffic Priority                      : 0
Maximum Sustained rate                : 100000 bits/sec
Maximum Burst                         : 3044 bytes
Minimum Reserved Rate                 : 0 bits/sec
Minimum Packet Size                   : 0 bytes

!Upstream Buffer Control Parameters
Minimum Buffer Size                   : 1000 bytes
Target Buffer Size                    : 1500 bytes
Maximum Buffer Size                   : 2000 bytes
Peak Rate                             : 0 bits/sec
Admitted QoS Timeout                  : 200 seconds
Active QoS Timeout                    : 0 seconds
Packets                               : 3
Bytes                                 : 1020
Rate Limit Delayed Grants             : 0
Rate Limit Dropped Grants             : 0
Current Throughput                    : 0 bits/sec, 0 packets/sec
Application Priority                  : 0
US Bonded                             : YES
Upstream Bonding Group                : UBG-1
Transmit Channel Set                  : 0x6
Sid Cluster                           : SC-0, Sid [ 10 10 ]
Segments Valid                        : 3
Segments Discarded                    : 0
Segments Lost                         : 0
SID Cluster Switching Information
Total Bytes Requested                 : 0
Total Time                            : 0
Outstanding Bytes                     : 0
Max Requests                          : 1
Classifiers: NONE
Sid                           : 10
Request polls issued          : 0
BWReqs {Cont,Pigg,RPoll,Other} : 4, 0, 0, 0
No grant buf BW request drops  : 0, where:0
Rate exceeded BW request drops : 0
Grants issued                 : 4
Packets received              : 4
```

```
Bytes received                 : 1488
rate-adapt                     : Disabled
rate-adapt {rcvd, Consec-PB}   : 0, 0
Fragment reassembly completed  : 0
Fragment reassembly incomplete : 0
Concatenated packets received  : 0
Queue-indicator bit statistics : 0 set, 0 granted
Good Codewords rx              : 8
Corrected Codewords rx         : 0
Uncorrectable Codewords rx     : 0
Concatenated headers received  : 0
Fragmentation headers received : 0
Fragmentation headers discarded: 0
ARP Requests Received          : 2
```

Additional References

MIBs

MIB	MIBs Link
DOCS-IF3-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configuring Upstream Cable Interface Features on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 12: Feature Information for Configuring Upstream Cable Interface Features on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Configuring Upstream Cable Interface Features on the Cisco CMTS Routers	12.2(33)SCA	This feature was introduced on the 12.2(33)SC release train.
Configuring Upstream Cable Interface Features on the Cisco CMTS Routers	12.2(33)SCD5	The Upstream Minimum Reserved Traffic Rate Plus Excess Traffic Rate featurette was introduced.
Upstream Buffer Control for Maximum Queue Depth	12.2(33)SCF2	This feature enables the Cisco CMTS to control the size of the upstream service-flow queue (or buffer) on a CM. The following commands were modified: • **cable service class** • **show cable modem service-flow** • **show cable service-class**
Copy and Paste Support for TDMA to A-TDMA Upgrade	12.2(33)SCG2	This feature automatically sets the DOCSIS mode to A-TDMA-only (DOCSIS 2.0) mode. The following command was modified: **cable upstream channel-width, cable upstream docsis-mode**
Upstream Drop Classifier (UDC)	12.2(33)SCG5	This feature enables the upstream drop classifier feature on the cable modems on a specific interface. The following commands were introduced or modified: **cable udc-capability**, **show cable modem verbose**

CHAPTER 11

Cable Modem Steering on the Cisco CMTS Routers

First Published: December 18, 2008

Last Updated: August 08, 2013

The cable modem steering feature helps to redirect or steer cable modems to multiple CMTS routers using downstream frequency overrides. A configurable string is used to bond the cable modem to the proper CMTS. Once the bonding is done, the CMTS can move the cable modem within itself for load balancing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Cable Modem Steering

DOCSIS 3.0-defined type, length, values (TLVs) are required to aid channel selection. All TLVs encoded as general extension information in cable modem configuration files are backward compatible with DOCSIS 1.1 and DOCSIS 2.0 cable modems.

The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 13: Cable Modem Steering Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [13]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [14]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

13 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
14 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Cable Modem Steering

The Cable Modem Steering feature has the following general restrictions:

- To restrict the cable modem on the exact downstream on the target CMTS, the redirection must be configured on the target CMTS.
- You must manually execute the **clear cable modem service-type** command to clear the cable modem service type identifier stored at the CMTS during registration.
- You must manually execute the **clear cable modem attribute-masks** command to clear the cable modem attribute masks stored at the CMTS during registration. These attribute masks are used to restrict usage of upstream channels during ranging time.
- cable modem steering supports only upstream masks.
- Channel steering does not take place when the cable modem fails in initial ranging.
- The cable modem will take more time to come online when channel steering is deployed. The time taken is proportional to the number of modems, and the downstreams and upstreams that the cable modem can reach.
- A modem cannot be load balanced to any upstream channel with attributes that conflict with attribute masks of the modem.
- The keep alive detection feature may trigger an line card (LC) switchover. For more details on the Keep Alive feature, see N+1 Redundancy for the Cisco Cable Modem Termination System.
- Each interface should have an active modem or use **no keepalive** on this interface.
- The required attribute mask and the forbidden attribute mask of an upstream should be configured in such a way that the bitwise AND of the two masks are zero. For example, if you configure required attribute mask with the value 0x30 and forbidden attribute mask with the value 0x20, the cable modem may not work properly, because the binary representation of both the configured masks will be 1 at the 5th bit.

Information About Cable Modem Steering

Cable modem steering allows you to redirect or steer the cable modems to one or more CMTS routers using downstream frequency overrides. Once a cable modem registers on a downstream on the proper CMTS router, the CMTS router can move the cable modem to any location for load balancing.

The DOCSIS 3.0-compliant Service Type Identifier used as the configurable string in the cable modem configuration file is backward-compatible with DOCSIS 1.1 and DOCSIS 2.0 cable modems.

The CMTS router can also impose restrictions on the number of channels a cable modem can use. DOCSIS 3.0 defines several TLVs to aid the channel selection.

The following TLVs are used in cable modem steering:

- TLV 43.9 (Cable Modem Attribute Masks) limits the set of channels the CMTS router can assign to the cable modem by allowing or forbidding certain binary attributes. The cable modem attribute masks have four sub-TLVs and cable modem steering makes use of two sub-TLVs, which are listed below:
  - TLV 43.9.3—Cable Modem Upstream Required Attribute Mask (C.1.1.18.1.8.3 of CM-SP-MULPIv3.0-I07-080215). It is a 32-bit mask representing the set of binary upstream channel attributes required for the cable modem.
  - TLV 43.9.4—Cable Modem Upstream Forbidden Attribute Mask (C.1.1.18.1.8.4 of CM-SP-MULPIv3.0-I07-080215). It is a 32-bit mask representing the set of binary upstream channel attributes forbidden for the cable modem.
- TLV 43.11 is used for a redirection action based on the service type identifier field. The cable modem sends the TLV 43.11 in the REG-REQ MAC message. The DOCSIS 1.1 and DOCSIS 2.0 modems will also send this file ID when doing the registration.
- TLV43.1, defined as Policy ID in DOCSIS 2.0 and DOCSIS 3.0, is parsed and stored in the cable modem during registration. Before moving the cable modem during load balancing (LB), the CMTS router checks whether the cable modem has a preconfigured policy with the same Policy ID. If the policy does exist, the CMTS router disables LB for this cable modem and moves to the next cable modem. If the policy does not exist on the CMTS router, or the Policy ID is missing from the cable modem configuration file, LB prohibition is not performed.

The following TLVs are supported in cable modem steering:

- TLV 43.11 (Service type identifier) from section C.1.1.18.1.10 in CM-SP-MULPIv3.0-I07-080215.
- Cable modem attribute masks (TLV 43.9) from C.1.1.18.1.8.3 and C.1.1.18.1.8.4 of CM-SP-MULPIv3.0-I07-080215.
- TLV portion (43.1, Policy ID) of REQ-REQ
- TLV 19---Channel Class ID
- TLV 18--- Ranging Hold-off Priority Field

Cable modem steering contains three small featurettes: Channel Redirection, Channel Restriction, and Load Balancing. The Load Balancing feature is covered in the Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers document .

Channel Redirection

The service type identifier-based channel redirection allows you to redirect or steer the cable modems to one or more CMTS routers using downstream frequency overrides. A configurable string in the cable modem configuration file is used to bond the cable modem to the correct CMTS router. A global CLI ties the string to the downstream frequency, which is configured on the CMTS router.

Once a cable modem registers on a downstream of a CMTS router, the CMTS router can move the cable modem to any location within the CMTS for load balancing.

A DOCSIS 3.0-compliant TLV (TLV 43.11) service identifier is used as the configurable string in the cable modem configuration file. It is backward-compatible with DOCSIS 1.1 and DOCSIS 2.0 cable modems. This TLV is used as the tag of the cable modem to decide whether to redirect or not. The method used to redirect is downstream frequency override in the ranging phase.

Channel Restriction

The Cisco CMTS router can impose restrictions on the channels a cable modem uses based on the cable modem configuration file or its capabilities. For example, Advanced Time Division Multiple Access (ATDMA) capable cable modems should not use Time Division Multiple Access (TDMA) upstream channels.

DOCSIS 3.0 provides guidelines on how a CMTS router can choose a pair of channels for a cable modem at both registration time and during autonomous load balancing. DOCSIS 3.0 defines several TLVs to aid channel selection, including the service type identifier, load balancing group ID, and cable modem attribute masks and service flow attribute masks.

Except for the service flow attribute masks, the TLVs are encoded as general extension information in the cable modem configuration file, which are backward compatible with DOCSIS 1.1 and DOCSIS 2.0 cable modems.

Channel restriction looks only for upstream cable modem attribute masks, and is therefore compatible with DOCSIS 1.1, DOCSIS 2.0 and DOCSIS 3.0 cable modems in non-Multiple Transmit Channel (MTC) mode.

Note In Cisco IOS Release 12.2(33)SCC and later releases, it is recommended to assign a cable modem to different Restricted Load Balancing Groups (RLBGs) to restrict the usage of channels, instead of using attribute masks.

Note In Cisco IOS Release 12.2(33)SCH1, the cable modems can come wideband online (w-online) with up to 16 downstream channels and 4 upstream channels. Effective with Cisco IOS Release 12.2(33)SCH2, the cable modems can come w-online with up to 24 downstream channels and 8 upstream channels. These features are not supported on the Cisco uBR10012 routers using PRE2, and the Cisco uBR7200 series routers using NPE-G1.

Upstream Channel Descriptor TLV for Ranging Hold-off

The Upstream Channel Descriptor (UCD) TLV for Ranging Hold-off feature, introduced in Cisco IOS Release 12.2(33)SCH, enables the CMTS router to hold off a cable modem from initial ranging based on TLV 18 and 19 specified in the upstream channel descriptor (UCD) messages. The router can hold off a cable modem from

initial ranging only for 5 minutes. This default value cannot be changed. This feature is supported with DOCSIS 2.0 and later releases cable modems using upstream logical channels.

Note The UCD TLV for Ranging Hold-off feature is supported only with DOCSIS load balance.

Ranging Class ID

The CMTS enables UCD TLV for ranging hold-off after detecting the TLVs from the cable modem registration request (REG-REQ) or multipart registration request (REG-REQ-MP), and saves these TLVs as a cable modem ranging class ID.

By default, DOCSIS load balance is supported for all cable modems with all types of ranging class IDs. In the event of DOCSIS load balance, a cable modem moves to the target upstream channel only if the ranging class ID matches with the upstream channel class ID.

Cable Modem Exclusion for DOCSIS Load Balance

You can exclude a cable modem or a group of cable modems from DOCSIS load balance based on their device type, MAC address, and Organizational Unique Identifier (OUI) using the **cable load-balance exclude** command in global configuration mode.

How to Configure Cable Modem Steering on the CMTS Router

This section describes the following required and optional procedures:

Configuring a Channel Redirection

To configure a channel redirection that allows you to redirect or steer the cable modems to one or more CMTS using the downstream frequency override in the ranging phase, use the **cable service type ds-frequency** command.

Restriction You can redirect cable modems matching the service type identifier to a downstream frequency. However, one service type identifier cannot be redirected to multiple downstream frequencies.

During registration, the cable modem service type identifier is stored in the CMTS to redirect target downstream frequency during ranging time. If you want to clear the stored service type identifier, you must manually execute the **clear cable modem service-type** command.

To restrict the cable modem on the exact downstream on the target CMTS, the redirection must be configured on the target CMTS. If the cable modems are redirected to the source CMTS, the dynamic load balance may not work properly and the cable modem may drop offline during load balancing. For the cable modems to be redirected it must reach the target frequency.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service type** *service-type-id* **ds-frequency** *frequency* **Example:** `Router(config)# cable service type commercial ds-frequency 519000000`	Redirects matching service types to downstream frequency. • *service-type-id*—Specifies the service type identifier to be redirected. Maximum length is 16. • *frequency*—Specifies the downstream frequency to which the cable modems are redirected.

Configuring a Channel Restriction

To impose restrictions on the channels a cable modem can use based on its configuration file or capabilities, use the **cable upstream attribute-mask** command.

Before You Begin

Advanced Time Division Multiple Access (ATDMA) capable cable modems should be restricted from using Time Division Multiple Access (TDMA) upstream channels.

Restriction

- The cable modem attribute masks (TLV 43.9) are a function of the CMTS support and are compatible only with legacy DOCSIS 1.1 and DOCSIS 2.0 cable modems.
- When the CMTS cannot find an appropriate US channel in the same legacy LB group, the cable modem steering checking is skipped and cable modems come online. The US channel must meet the requirement of cable modem upstream attribute masks if a load balancing group (LBG) is not configured.
- During registration, the cable modem attribute masks are stored at the CMTS. These are then used to restrict usage of upstream channels during ranging time. You must manually execute the **clear cable modem attribute-masks** command to clear the stored attribute masks.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/subslot/port* **Example:** `Router(config)# interface cable 5/0/4`	Enables the cable interface.
Step 4	**cable upstream** *upstream-interface* **attribute-mask** *attribute-mask* **Example:** `Router(config-if)# cable upstream 0 attribute-mask ffff`	Configures the attribute mask on a particular upstream interface. • *upstream-interface*—Specifies the upstream port. • *attribute-mask*—Specifies the attribute mask bitmap in hexadecimal format. Example: 0-FFFFFFFF **Note** From Cisco IOS Release 12.2(33)SCC, the bit 0 in *attribute-mask* is bypassed when cable modem steering checks it.

Configuring an Upstream Channel Class ID

This configuration is optional. A channel class ID must be configured for an upstream logical channel if you want to configure UCD TLV ranging hold-off on the CMTS router.

Restriction Legacy load balance cannot be configured on a MAC domain if an upstream channel belonging to the MAC domain has a channel class ID configured. Similarly, a channel class ID cannot be configured on an upstream channel if legacy load balance is already configured on the MAC domain of the upstream channel.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/subslot/cable-interface-index* **Example:** `Router(config)# interface cable 5/0/4`	Specifies the cable interface and enters cable interface configuration mode. Arguments for this command may vary depending on the CMTS router, line card, and Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *Slot*—Slot where a line card resides. • *Subslot* (Cisco uBR10012 only)—Secondary slot number of a line card. • *cable-interface-index*—Downstream port or MAC domain index of a line card.
Step 4	**cable upstream** *port-number* **chan-class-id** *id* **Example:** `Router(config-if)# cable upstream 0 chan-class-id ff`	Configures the channel class ID for an upstream logical channel. • *port-number*—Cable upstream port number. The valid range depends on the number of upstream channels configured in a MAC domain. For example, if the total number of upstream channels configured is 4, then the valid range for the upstream port number is from 0 to 3. • *id*—Channel class ID for the logical upstream channel in the hexadecimal format. The valid range is from 0 to ffffffff. The default value is 0.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring an Upstream Ranging Hold-off Priority Value

This configuration is optional.

Maximum time that a cable modem can inhibit transmissions on an upstream channel in response to its ranging class ID matching a bit value in the Ranging Hold-off Priority field in the cable modem configuration file is 300 seconds (five minutes) per *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification* . This default timer value cannot be changed.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/subslot/cable-interface-index* **Example:** `Router(config)# interface cable 5/0/4`	Specifies the cable interface and enters cable interface configuration mode. Arguments for this command may vary depending on the CMTS router, line card, and Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *Slot*—Slot where a line card resides. • *Subslot* (Cisco uBR10012 only)—Secondary slot number of a line card. • *cable-interface-index*—Downstream port or MAC domain index of a line card.
Step 4	**cable upstream** *port-number* **rng-holdoff** *priority* **Example:** `Router(config-if)# cable upstream 0 rng-holdoff 1`	Configures the ranging hold-off priority value for an upstream logical channel. • *port-number*—Upstream port number. The valid range depends on the number of upstream channels configured in a MAC domain. For example, if the total number of upstream channels configured is 4, then the valid range for the upstream port number is from 0 to 3. • **rng-holdoff** *priority*—Specifies the ranging hold-off priority value in the hexadecimal format. The valid range is from 0 to ffffffff. The default value is 0.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Cable Modem Steering

This section provides the following configuration examples:

Example: Configuring a Channel Class ID and Ranging Hold-off Priority Value

The following example shows configuration of a channel class ID and its ranging hold-off priority value on a cable interface line card on the Cisco uBR10012 router:

```
interface Cable8/1/0
downstream Integrated-Cable 8/1/0 rf-channel 0-3
```

```
cable mtc-mode
no cable packet-cache
cable bundle 1
cable upstream max-ports 4
cable upstream bonding-group 1
  upstream 1
  upstream 2
  upstream 3
  attributes 80000000
cable upstream bonding-group 2
  upstream 0
  upstream 2
  upstream 3
  attributes 80000000
cable upstream bonding-group 3
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes 80000000
cable upstream 0 connector 0
cable upstream 0 frequency 24400000
cable upstream 0 channel-width 1600000 1600000
cable upstream 0 max-logical-chans 1
cable upstream 0 docsis-mode atdma
cable upstream 0 minislot-size 4
cable upstream 0 range-backoff 3 6
cable upstream 0 modulation-profile 221
cable upstream 0 chan-class-id FF
cable upstream 0 rng-holdoff F
no cable upstream 0 shutdown
cable upstream 1 connector 1
cable upstream 1 frequency 22800000
cable upstream 1 channel-width 1600000 1600000
cable upstream 1 max-logical-chans 1
cable upstream 1 docsis-mode atdma
cable upstream 1 minislot-size 4
cable upstream 1 range-backoff 3 6
cable upstream 1 modulation-profile 221
cable upstream 1 chan-class-id F
```

Example: Clearing a Channel Redirection

To clear the cable modem attributes, use the **clear cable modem** command as shown in the following examples:

```
Router# clear cable modem all
Router# clear cable modem oui string
Router# clear cable modem cable slot/subslot/port offline
```

To clear the cable modem service type identifiers, use the **clear cable modem service-type** command as shown in the following examples:

```
Router# clear cable modem all service-type-id
Router# clear cable modem oui string service-type-id
Router# clear cable modem slot/subslot/port offline service-type-id
```

Verifying and Troubleshooting Cable Modem Steering

This section provides the verification and troubleshooting information:

Verifying a Channel Redirection

To verify configuration of channel redirection, use the **show cable modem verbose** command as shown in the following example:

```
Router# show cable modem verbose

MAC Address                          : 0019.474d.e291
IP Address                           : 41.42.0.0
IPv6 Address                         : ---
Dual IP                              : N
Prim Sid                             : 15
Host Interface                       : C5/0/4/U0
MD-DS-SG                             : N/A
Wideband Capable                     : Y
RCP Index                            : 0
sysDescr                             :
Upstream Power                       : 0.00 dBmV (SNR = 36.12 dB)
Downstream Power                     : 0.00 dBmV (SNR = ----- dB)
Timing Offset                        : 1874
Initial Timing Offset                : 1874
Curr US Timing Adjust                : 0
Prev US Timing Adjust                : 0
Received Power                       :  0.00 dBmV
MAC Version                          : DOC2.0
QoS Provisioned Mode                 : DOC1.1
Enable DOCSIS2.0 Mode                : Y
Phy Operating Mode                   : tdma
Modem Status                         : {Modem=online(pt), Security=assign(tek)}
Capabilities                         : {Frag=Y, Concat=Y, PHS=Y}
Security Capabilities                : {Priv=BPI+, EAE=N}
L2VPN Capabilities                   : {L2VPN=N, eSAFE=N}
Sid/Said Limit                       : {Max US Sids=16, Max DS Saids=15}
Optional Filtering Support           : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support           : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE IPs                    : 0(Max CPE IPs = 16)
CFG Max-CPE                          : 10
Flaps                                : 0()
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 0 aborts, 0 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 1 packets, 401 bytes
Total US Throughput                  : 0 bits/sec, 0 packets/sec
Total DS Data                        : 0 packets, 0 bytes
Total DS Throughput                  : 0 bits/sec, 0 packets/sec
LB group index                       : 0x0
LB reg_group_id                      : 0x0
LB policy id                         : 0
LB reg_policy_id                     : 0
LB priority                          : 0
Required DS Attribute Mask           : 0x0
Forbidden DS Attribute Mask          : 0x0
Required US Attribute Mask           : 0x0
Forbidden US Attribute Mask          : 0x0
Service Type ID                      : commercial
Active Classifiers                   : 0 (Max = NO LIMIT)
DSA/DSX messages                     : permit all
Number of Multicast DSIDs Support    : 15
MDF Capability Mode                  : 0
FCType10 Forwarding Support          : N
Features Bitmask                     : 0x0
Total Time Online                    : 00:59
```

To view the modems having the service type identifier, use the **show cable modem service-type** *service-type-id* command as shown in the following example:

```
Router# show cable modem service-type commercial
                                                                        B D
MAC Address    IP Address      I/F       MAC         Prim Service-type-id    P I
```

```
                                        State       Sid                    I  P
0018.6812.29ae 41.42.2.212    C5/0/4/U2 offline     3838 commercial        N  N
0018.6811.f9f8 41.42.0.140    C5/0/4/U2 offline     3225 commercial        N  N
0018.6811.fba6 41.42.5.169    C5/0/4/U2 offline     3439 commercial        N  N
0018.6812.225a 41.42.3.210    C5/0/4/U2 offline     3355 commercial        N  N
0018.6811.fa8c 41.42.1.133    C5/0/4/U2 offline     3091 commercial        N  N
0018.6812.37e8 41.42.0.136    C5/0/4/U2 offline     7439 commercial        N  N
0018.6811.fbca 41.42.2.255    C5/0/4/U2 offline     6263 commercial        N  N
0018.6811.fb44 41.42.2.17     C5/0/4/U2 offline     2996 commercial        N  N
0018.6812.2f20 41.42.0.100    C5/0/4/U2 offline     3544 commercial        N  N
```

Verifying a Channel Restriction

To verify the service type identifier and cable modem attribute masks configured for a cable modem, use the **show cable modem verbose** command as shown in the following example:

```
Router# show cable modem 0019.474d.e291 verbose

MAC Address                          : 0019.474d.e291
IP Address                           : 40.3.100.16
IPv6 Address                         : ---
Dual IP                              : N
Prim Sid                             : 35
Host Interface                       : C5/0/4/U0
MD-DS-SG                             : 1
MD-CM-SG                             : 0x40100
Primary Downstream                   : Mo1/0/0:0 (RfId : 0)
Wideband Capable                     : N
RCP Index                            : 0
sysDescr                             :
Upstream Power                       : 0.00 dBmV (SNR = 36.12 dB)
Downstream Power                     : 0.00 dBmV (SNR = ----- dB)
Timing Offset                        : 1573
Initial Timing Offset                : 1573
Curr US Timing Adjust                : 0
Prev US Timing Adjust                : 0
Received Power                       :  -0.50 dBmV
MAC Version                          : DOC2.0
QoS Provisioned Mode                 : DOC1.1
Enable DOCSIS2.0 Mode                : Y
Phy Operating Mode                   : tdma
Modem Status                         : {Modem=online, Security=disabled}
Capabilities                         : {Frag=Y, Concat=Y, PHS=Y}
Security Capabilities                : {Priv=, EAE=N}
L2VPN Capabilities                   : {L2VPN=N, eSAFE=N}
Sid/Said Limit                       : {Max US Sids=16, Max DS Saids=15}
Optional Filtering Support           : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support           : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE IPs                    : 0(Max CPE IPs = 16)
CFG Max-CPE                          : 16
Flaps                                : 0()
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 0 aborts, 0 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 7 packets, 619 bytes
Total US Throughput                  : 0 bits/sec, 0 packets/sec
Total DS Data                        : 2 packets, 148 bytes
Total DS Throughput                  : 4 bits/sec, 0 packets/sec
LB group index                       : 0x0
LB reg_group_id                      : 0x0
LB policy id                         : 2
LB reg_policy_id                     : 2
LB priority                          : 0
Required DS Attribute Mask           : 0x0
Forbidden DS Attribute Mask          : 0x0
Required US Attribute Mask           : 0x1111
Forbidden US Attribute Mask          : 0x0
Service Type ID                      : commercial
Active Classifiers                   : 0 (Max = NO LIMIT)
```

```
DSA/DSX messages                    : permit all
Voice Enabled                       : NO
DS Change Times                     : 0
Boolean Services                    : 0
Number of Multicast DSIDs Support   : 0
MDF Capability Mode                 : 0
FCType10 Forwarding Support         : N
Features Bitmask                    : 0x0
Total Time Online                   : 00:19
```

Verifying an Upstream Ranging Class ID Configuration

To verify an upstream ranging class ID of a cable modem, use the **show cable modem** command with the **verbose** keyword.

Following is a sample output of the **show cable modem verbose** command in Cisco IOS Release 12.2(33)SCH1:

```
Router# show cable modem 68b6.fcfe.2285 verbose

MAC Address : 68b6.fcfe.2285
IP Address : 192.168.0.8
IPv6 Address : 2001:DB8:10:1:9951:1972:33F9:9867
Dual IP : Y
Prim Sid : 235
Host Interface : C7/0/1/UB
MD-DS-SG / MD-US-SG : 1 / 1
MD-CM-SG : 0x3D0101
Primary Wideband Channel ID : 2305 (Wi7/0/0:0)
Primary Downstream : In7/0/0:3 (RfId : 1731)
Wideband Capable : Y
RCP Index : 3
RCP ID : 00 10 00 00 18
Downstream Channel DCID RF Channel : 117 7/0/0:0
Downstream Channel DCID RF Channel : 118 7/0/0:1
Downstream Channel DCID RF Channel : 119 7/0/0:2
Downstream Channel DCID RF Channel : 120 7/0/0:3
Downstream Channel DCID RF Channel : 121 7/0/1:0
Downstream Channel DCID RF Channel : 122 7/0/1:1
Downstream Channel DCID RF Channel : 123 7/0/1:2
Downstream Channel DCID RF Channel : 124 7/0/1:3
Downstream Channel DCID RF Channel : 125 7/0/2:0
Downstream Channel DCID RF Channel : 126 7/0/2:1
Downstream Channel DCID RF Channel : 127 7/0/2:2
Downstream Channel DCID RF Channel : 128 7/0/2:3
Downstream Channel DCID RF Channel : 129 7/0/3:0
Downstream Channel DCID RF Channel : 130 7/0/3:1
Downstream Channel DCID RF Channel : 131 7/0/3:2
Downstream Channel DCID RF Channel : 132 7/0/3:3
Extended Upstream Transmit Power : 61dB
Multi-Transmit Channel Mode : Y
Number of US in UBG : 4
Upstream Channel : US0 US1 US2 US3
Ranging Status : sta sta sta sta
Upstream SNR (dB) : 36.12 36.12 36.12 36.12
Upstream Data SNR (dB) : -- -- -- --
Received Power (dBmV) : -0.50 -0.50 0.00 -0.50
Reported Transmit Power (dBmV) : 38.25 38.25 38.25 38.25
Peak Transmit Power (dBmV) : 61.00 61.00 61.00 61.00
Phy Max Power (dBmV) : 51.00 51.00 51.00 51.00
Minimum Transmit Power (dBmV) : 24.00 24.00 24.00 24.00
Timing Offset (97.6 ns): 1348 1348 1348 1348
Initial Timing Offset : 1092 1092 1092 1348
Rng Timing Adj Moving Avg(0.381 ns): 0 0 -1 0
Rng Timing Adj Lt Moving Avg : 644 737 644 0
Rng Timing Adj Minimum : 0 0 -256 0
Rng Timing Adj Maximum : 65536 65536 65536 256
Pre-EQ Good : 0 0 0 0
Pre-EQ Scaled : 0 0 0 0
Pre-EQ Impulse : 0 0 0 0
Pre-EQ Direct Loads : 0 0 0 0
```

```
Good Codewords rx : 25 30 36 67
Corrected Codewords rx : 0 0 0 0
Uncorrectable Codewords rx : 0 0 0 0
Phy Operating Mode : atdma* atdma* atdma* atdma*
sysDescr :
Downstream Power : 0.00 dBmV (SNR = ----- dB)
MAC Version : DOC3.0
QoS Provisioned Mode : DOC1.1
Enable DOCSIS2.0 Mode : Y
Modem Status : {Modem= w-online, Security=disabled}
Capabilities : {Frag=N, Concat=N, PHS=Y}
Security Capabilities : {Priv=, EAE=Y, Key_len=}
L2VPN Capabilities : {L2VPN=Y, eSAFE=Y}
Sid/Said Limit : {Max US Sids=8, Max DS Saids=64}
Optional Filtering Support : {802.1P=N, 802.1Q=N, DUT=Y}
Transmit Equalizer Support : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE : 1(Max CPE = 16)
Number of CPE IPs : 0(Max CPE IPs = 16)
CFG Max-CPE : 16
Flaps : 0()
Errors : 0 CRCs, 0 HCSes
Stn Mtn Failures : 0 aborts, 0 exhausted
Total US Flows : 1(1 active)
Total DS Flows : 1(1 active)
Total US Data : 29 packets, 8048 bytes
Total US Throughput : 0 bits/sec, 0 packets/sec
Total DS Data : 1 packets, 275 bytes
Total DS Throughput : 0 bits/sec, 0 packets/sec
LB group ID assigned (index) : 2151481601 (48385)
LB group ID in config file (index) : N/A (N/A)
LB policy ID : 0
LB policy ID in config file : 0
LB priority : 0
Tag :
Required DS Attribute Mask : 0x0
Forbidden DS Attribute Mask : 0x0
Required US Attribute Mask : 0x0
Forbidden US Attribute Mask : 0x0
Service Type ID :
Service Type ID in config file :
Ranging Class ID : 0x2
Active Classifiers : 0 (Max = NO LIMIT)
CM Upstream Filter Group : 0
CM Downstream Filter Group : 0
CPE Upstream Filter Group : 0
CPE Downstream Filter Group : 0
DSA/DSX messages : permit all
Voice Enabled : NO
DS Change Times : 0
Boolean Services : 2
Number of Multicast DSIDs Support : 63
MDF Capability Mode : 2
IGMP/MLD Version : MLDv2
FCType10 Forwarding Support : Y
Features Bitmask : 0x0
Total Time Online : 08:06 (08:06 since last counter reset)
CM Initialization Reason : T4_EXPIRED
CFG Max IPv6 CPE Prefix : 16 (-1 used)
```

Following is a sample output of the **show cable modem verbose** command in Cisco IOS Release 12.2(33)SCH2:

```
Router# show cable modem 68b6.fcfe.22e5 verbose

MAC Address                     : 68b6.fcfe.22e5
IP Address                      : 192.168.0.8
IPv6 Address                    : 2001:DB8:10:1:9951:1972:33F9:9867
Dual IP                         : Y
Prim Sid                        : 8
Host Interface                  : C8/0/0/UB
MD-DS-SG / MD-US-SG             : 1 / 2
MD-CM-SG                        : 0x5A0102
Primary Wideband Channel ID     : 3073 (Wi8/0/0:0)
Primary Downstream              : Mo8/0/0:0 (RfId : 2304)
```

```
Wideband Capable                    : Y
RCP Index                           : 3
RCP ID                              : 00 10 00 00 18
Downstream Channel DCID RF Channel : 45    8/0/0:0
Downstream Channel DCID RF Channel : 46    8/0/0:1
Downstream Channel DCID RF Channel : 47    8/0/0:2
Downstream Channel DCID RF Channel : 48    8/0/0:3
Downstream Channel DCID RF Channel : 49    8/0/0:4
Downstream Channel DCID RF Channel : 50    8/0/0:5
Downstream Channel DCID RF Channel : 51    8/0/0:6
Downstream Channel DCID RF Channel : 52    8/0/0:7
Downstream Channel DCID RF Channel : 53    8/0/0:8
Downstream Channel DCID RF Channel : 54    8/0/0:9
Downstream Channel DCID RF Channel : 55    8/0/0:10
Downstream Channel DCID RF Channel : 56    8/0/0:11
Downstream Channel DCID RF Channel : 57    8/0/0:12
Downstream Channel DCID RF Channel : 58    8/0/0:13
Downstream Channel DCID RF Channel : 59    8/0/0:14
Downstream Channel DCID RF Channel : 60    8/0/0:15
Downstream Channel DCID RF Channel : 61    8/0/0:16
Downstream Channel DCID RF Channel : 62    8/0/0:17
Downstream Channel DCID RF Channel : 63    8/0/0:18
Downstream Channel DCID RF Channel : 64    8/0/0:19
Downstream Channel DCID RF Channel : 65    8/0/0:20
Downstream Channel DCID RF Channel : 66    8/0/0:21
Downstream Channel DCID RF Channel : 67    8/0/0:22
Downstream Channel DCID RF Channel : 68    8/0/0:23
UDC Enabled                         : N
Extended Upstream Transmit Power    : 61dB
Multi-Transmit Channel Mode         : Y
Number of US in UBG                 : 8
Upstream Channel                    : US0        US1        US2        US3
Ranging Status                      : sta        sta        sta        sta
Upstream SNR (dB)                   : 30.62      32.32      18.25      24.26
Upstream Data SNR (dB)              : --         --         --         --
Received Power (dBmV)               : 0.50       0.00       -0.50      -0.50
Reported Transmit Power (dBmV)      : 30.75      30.75      29.25      29.25
Peak Transmit Power (dBmV)          : 61.00      61.00      61.00      61.00
Phy Max Power (dBmV)                : 48.00      48.00      48.00      48.00
Minimum Transmit Power (dBmV)       : 21.00      21.00      21.00      21.00
Timing Offset              (97.6 ns): 1800       1800       1800       1800
Initial Timing Offset               : 1544       1544       1544       1544
Rng Timing Adj Moving Avg(0.381 ns): -1         0          -1         -1
Rng Timing Adj Lt Moving Avg        : -7         0          -7         -7
Rng Timing Adj Minimum              : -256       0          -256       -256
Rng Timing Adj Maximum              : 65536      65536      65536      65536
Pre-EQ Good                         : 0          0          0          0
Pre-EQ Scaled                       : 0          0          0          0
Pre-EQ Impulse                      : 0          0          0          0
Pre-EQ Direct Loads                 : 0          0          0          0
Good Codewords rx                   : 1201       1262       833        656
Corrected Codewords rx              : 0          0          169        117
Uncorrectable Codewords rx          : 0          0          205        335
Phy Operating Mode                  : atdma*     atdma*     atdma*     atdma*
Upstream Channel                    : US4        US5        US6        US7
Ranging Status                      : sta        sta        sta        sta
Upstream SNR (dB)                   : 15.53      31.62      31.1       31.87
Upstream Data SNR (dB)              : --         --         --         --
Received Power (dBmV)               : 0.00       0.00       -0.50      0.50
Reported Transmit Power (dBmV)      : 29.25      30.75      30.75      30.75
Peak Transmit Power (dBmV)          : 61.00      61.00      61.00      61.00
Phy Max Power (dBmV)                : 48.00      48.00      48.00      48.00
Minimum Transmit Power (dBmV)       : 21.00      21.00      21.00      21.00
Timing Offset              (97.6 ns): 1800       1800       1800       1800
Initial Timing Offset               : 1544       1800       1544       1544
Rng Timing Adj Moving Avg(0.381 ns): -1         -1         46         0
Rng Timing Adj Lt Moving Avg        : -7         -7         104        0
Rng Timing Adj Minimum              : -256       -256       0          0
Rng Timing Adj Maximum              : 65536      256        65536      65536
Pre-EQ Good                         : 0          0          0          0
Pre-EQ Scaled                       : 0          0          0          0
Pre-EQ Impulse                      : 0          0          0          0
Pre-EQ Direct Loads                 : 0          0          0          0
```

```
Good Codewords rx                   : 718        1328       1173       1252
Corrected Codewords rx              : 110        0          0          0
Uncorrectable Codewords rx          : 298        0          0          0
Phy Operating Mode                  : atdma*     atdma*     atdma*     atdma*
sysDescr                            : DOCSIS 3.0 Cable Modem Router
Downstream Power                    : 7.40 dBmV (SNR = 43.30 dB)
MAC Version                         : DOC3.0
QoS Provisioned Mode                : DOC1.1
Enable DOCSIS2.0 Mode               : Y
Modem Status                        : {Modem= w-online, Security=disabled}
Capabilities                        : {Frag=N, Concat=N, PHS=Y}
Security Capabilities               : {Priv=, EAE=Y, Key_len=}
L2VPN Capabilities                  : {L2VPN=Y, eSAFE=Y}
Sid/Said Limit                      : {Max US Sids=8, Max DS Saids=64}
Optional Filtering Support          : {802.1P=N, 802.1Q=N, DUT=Y}
Transmit Equalizer Support          : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE                       : 0(Max CPE = 16)
Number of CPE IPs                   : 0(Max CPE IPs = 16)
Number of CPE IPv6                  : 0(Max CPE IPv6 = 16)
CFG Max-CPE                         : 16
Flaps                               : 19(Oct 11 04:00:25)
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 0 aborts, 12 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 3294 packets, 577031 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 2263 packets, 200777 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
LB group ID assigned (index)        : 2153382146 (55810)
LB group ID in config file (index) : N/A (N/A)
LB policy ID                        : 0
LB policy ID in config file         : 0
LB priority                         : 0
Tag                                 :
Required DS Attribute Mask          : 0x0
Forbidden DS Attribute Mask         : 0x0
Required US Attribute Mask          : 0x0
Forbidden US Attribute Mask         : 0x0
Service Type ID                     :
Service Type ID in config file      :
Ranging Class ID                    : 0x2
Active Classifiers                  : 0 (Max = NO LIMIT)
CM Upstream Filter Group            : 0
CM Downstream Filter Group          : 0
CPE Upstream Filter Group           : 0
CPE Downstream Filter Group         : 0
DSA/DSX messages                    : permit all
Voice Enabled                       : NO
DS Change Times                     : 0
Boolean Services                    : 2
Number of Multicast DSIDs Support   : 63
MDF Capability Mode                 : 2
IGMP/MLD Version                    : MLDv2
FCType10 Forwarding Support         : Y
Features Bitmask                    : 0x0
Total Time Online                   : 9h27m   (9h27m    since last counter reset)
CM Initialization Reason            : BAD_DHCP_ACK
CFG Max IPv6 CPE Prefix             : 16 (-1 used)
```

Clearing Attribute Masks

If the cable modem fails to come online after configuring attribute masks in the cable modem configuration file, you can use the following procedure to verify the contents of the cable modem configuration file and clear its contents if the attribute masks are configured differently.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable modem verbose** **Example:** `Router# show cable modem verbose`	Verifies whether the cable modem attribute masks have been configured in the cable modem configuration file. **Note** If the cable modem configuration file shows any change, use the **clear cable modem attribute-masks** command.
Step 3	**clear cable modem attribute-masks** **Example:** `Router# clear cable modem all attribute-masks`	Clears the cable modem attribute masks stored in CMTS.
Step 4	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration. Use it to verify whether upstream masks of the cable modem are configured on the corresponding upstream channel.

Debugging Channel Redirection

Use the following steps to debug channel redirection:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running config** **Example:** `Router# show running config`	Displays the running configuration. **Note** You can use this information to verify the CMTS configuration to make sure that the cable modems can reach the configured downstream-frequency.
Step 3	**debug cable range** **Example:** `Router# debug cable range`	Displays ranging messages from cable modems on the Hybrid Fiber-Coaxial (HFC) network.

	Command or Action	Purpose
Step 4	**debug cable registration** **Example:** `Router# debug cable registration`	Displays debug messages for the cable modem registration process.
Step 5	**debug cable mac-address** *mac* **verbose** **Example:** `Router# debug cable mac-address 00E0.1E00.0000 ffff.ff00.0000 verbose`	Displays debug information for a specific cable modem.
Step 6	**clear cable modem** *mac* **delete** **Example:** `Router# clear cable modem 00E0.1E00.0000 ffff.ff00.0000 delete`	Removes the specified modem from the CMTS. **Note** This allows the CMTS to re-register the cable modem's page.

Troubleshooting Tips

This section provides tips and commands you can use to troubleshoot your cable modem steering configuration.

- Clearing Attribute Masks, on page 277
- Debugging Channel Redirection, on page 278
- Because empty rules are not allowed, if you remove the last rule of a policy, using **no cable load-balance docsis-policy** *policy-id* **rule** *rule-id* or **no cable load-balance rule** *rule-id,* the policy itself will be removed.
- Use the **show running | include docsis-policy** command or the **show running-config | include rule** command to see the policy and rule configured in the system.

Additional References

The following sections provide references related to the Cable Modem Steering feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
DOCSIS 1.1 as it relates to Cisco CMTS	Cisco IOS CMTS Cable Software Configuration Guide
Load Balancing and Dynamic Channel Change (DCC)	Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers

Related Topic	Document Title
N+1 Redundancy	N+1 Redundancy for the Cisco Cable Modem Termination System

Standards and RFCs

Standard	Title
CM-SP-MULPIv3.0-I07-080215	DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification
CM-SP-MULPIv3.0-I18-120329	DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification
CM-SP-RFI2.0-I13-080215	DOCSIS 2.0 Radio Frequency Interface Specification

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Modem Steering

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

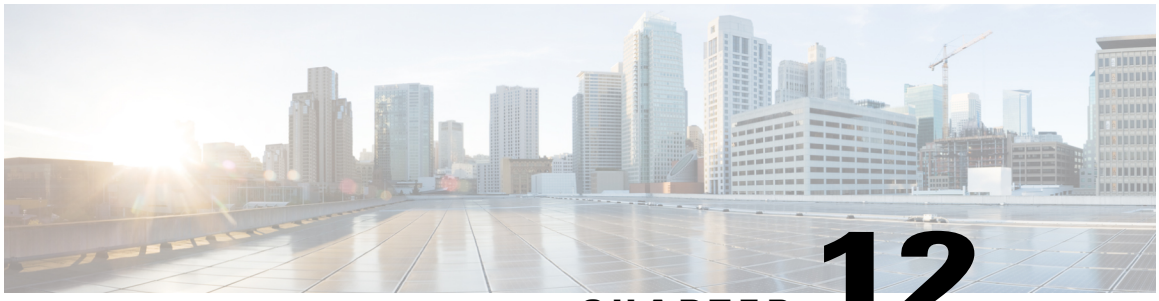
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 14: Feature Information for Cable Modem Steering on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Channel Redirection	12.2(33)SCB	Channel redirection allows you to redirect or steer the cable modems to one or more CMTS using downstream overrides. The following sections provide information about this feature: • Channel Redirection, on page 265 • Configuring a Channel Redirection, on page 266 • Verifying a Channel Redirection, on page 272 The following commands were introduced or modified: • **cable service type** • **cable service type ds-frequency** • **clear cable modem attribute-masks** • **clear cable modem service-type** • **show cable modem service-type-id**

Feature Name	Releases	Feature Information
Channel Restriction	12.2(33)SCB	The CMTS can impose restrictions on the channels a cable modem can use based on the cable modem configuration file or its capabilities. The following sections provide information about this feature: • Channel Restriction, on page 265 • Configuring a Channel Restriction, on page 267 • Verifying a Channel Restriction, on page 273 The following command is introduced: **cable upstream attribute-mask**.
Channel Restriction	12.2(33)SCB4	When the CMTS cannot find an appropriate US channel in the same legacy LB group, the cable modem steering checking is skipped and cable modems come online. The following sections provide information about this feature: • Configuring a Channel Restriction, on page 267
RLBG/GLBG Support and NB DBS Interact with DLB Support	12.2(33)SCC	The following sections have been updated with information about this feature: • Channel Restriction, on page 265 • Configuring a Channel Restriction, on page 267

Feature Name	Releases	Feature Information
UCD TLV for Ranging Hold-off	12.2(33)SCH	The UCD TLV for Ranging Hold-off feature enables the CMTS router to hold off a cable modem from initial ranging. The following sections provide information about this feature: • Upstream Channel Descriptor TLV for Ranging Hold-off, on page 265 • Configuring an Upstream Channel Class ID, on page 268 • Configuring an Upstream Ranging Hold-off Priority Value , on page 269 The following commands were introduced or modified: • **cable load-balance exclude** • **cable upstream chan-class-id** • **cable upstream rng-holdoff** • **show cable modem verbose**
16x4 Cable Modem Support	12.2(33)SCH1	The cable modems can come w-online with up to 16 downstream channels and 4 upstream channels. The following section provides information about this feature: • Channel Restriction, on page 265
24x8 Cable Modem Support	12.2(33)SCH2	The cable modems can come w-online with up to 24 downstream channels and 8 upstream channels. The following section provides information about this feature: • Channel Restriction, on page 265



CHAPTER 12

DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 11, 2012

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the DOCSIS 2.0 A-TDMA services feature, which provides support for DOCSIS 2.0 Advanced Time Division Multiple Access (A-TDMA) upstream modulation profiles on the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U Broadband Processing Engine (BPE) cable interface line cards. This feature supplements the existing support for DOCSIS 1.0 and DOCSIS 1.1 Time Division Multiple Access (TDMA) modulation profiles.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers

The table below shows the hardware compatibility prerequisites for this feature.

Table 15: DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(15)BC 2and later releases • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCA • PRE-2 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.3(15)BC2 and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(15)CX and 12.2(15)BC2 and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(15)CX and 12.2(15)BC2 and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

- The cable physical plant must be capable of supporting the higher-bandwidth DOCSIS 2.0 A-TDMA modulation profiles.
- Cable modems must be DOCSIS-compliant. If cable modems go offline, or appear to be online but do not pass traffic when in the mixed TDMA/A-TDMA mode, upgrade the modem software to a DOCSIS-compliant version.
- The following are required to support the DOCSIS 2.0 A-TDMA features:
  - Cable modems must be DOCSIS 2.0 capable.
  - The DOCSIS configuration file for a DOCSIS 2.0 cable modem must either omit the DOCSIS 2.0 Enable field (TLV 39), or it must set TLV 39 to 1 (enable). If you set TLV 39 to 0 (disable), a DOCSIS 2.0 CM uses the TDMA mode.
  - The upstream must be configured for either A-TDMA-only or mixed TDMA/A-TDMA mode. To use the 6.4 MHz channel width, the upstream must be configured for A-TDMA-only mode.
- Complete a basic configuration of the Cisco uBR7246VXR or Cisco uBR10012 router; this includes, at a minimum, the following tasks:
  - Configure a host name and password for the router.
  - Configure the router to support Internet Protocol (IP) operations.
  - Install and configure at least one WAN adapter to provide backbone connectivity.
- Determine a channel plan for your Cisco uBR7246VXR or Cisco uBR10012 router and all of its cable interfaces.
- Verify that your headend site includes all necessary servers to support DOCSIS and Internet connectivity, including DHCP, ToD, and TFTP servers.
- The system clock on the Cisco uBR7246VXR or Cisco uBR10012 router should be set to a current date and time to ensure that system logs have the proper timestamp and to ensure that the BPI+ subsystem uses the correct timestamp for verifying cable modem digital certificates.

Restrictions for DOCSIS 2.0 A-TDMA Services

- Does not support virtual channels, as described in DOCSIS 2.0 specification.
- Does not support Synchronous Code Division Multiple Access (S-CDMA) channels.

- Cisco IOS Release 12.2(15)CX, Release 12.2(15)BC2, and later releases support a maximum of 10 modulation profiles for each of the three DOCSIS modes (DOCSIS 1.x TDMA, mixed, and DOCSIS 2.0 A-TDMA), for a total maximum of 30 modulation profiles.
- Advanced hardware-based spectrum management is not supported for DOCSIS 2.0 mixed-mode and A-TDMA upstreams. Advanced spectrum management features (such as guided frequency hopping, dynamic upstream modulation, and proactive CNR-based frequency hopping and channel width changes) can be configured only on DOCSIS and EuroDOCSIS 1.X upstreams. You cannot use these features on channels configured for mixed mode or DOCSIS 2.0 A-TDMA mode. Advanced hardware-based spectrum management for A-TDMA operations is scheduled to be supported in a future release of the Cisco IOS software.
- Changing the DOCSIS mode of an upstream takes all cable modems on that upstream offline, which forces the cable modems to reregister, so that the CMTS can determine the capabilities of the cable modems on the new channels.

Information About DOCSIS 2.0 A-TDMA Services

DOCSIS 2.0 A-TDMA services 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.

In Cisco IOS Release 12.2(15)BC2, DOCSIS 2.0 A-TDMA services are supported on the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U Broadband Processing Engine (BPE) cable interface line cards.

DOCSIS 2.0 A-TDMA services incorporate 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, while retaining support for existing 16-QAM and QPSK modulation profiles. In addition, an 8-QAM modulation profile is supported for special applications.
- Supports a minislot size of 1 tick for A-TDMA operations.
- Increases channel widths to 6.4 MHz (5.12 Msymbol rate) for A-TDMA operations.
- A-TDMA and mixed modes of operation provide a more robust operating environment with increased protection against ingress noise and other signal impairments, using a number of new features:
  - Uses to a symbol (T)-spaced adaptive equalizer structure to increase the equalizer tap size to 24 taps, compared to 8 taps in DOCSIS 1.x mode. This allows operation in the presence of more severe multipath and microreflections, and can accommodate operation near band edges where group delay could be a problem.
  - Supports new QPSK0 and QPSK1 preambles, which provide improved burst acquisition by performing simultaneous acquisition of carrier and timing lock, power estimates, equalizer training, and constellation phase lock. This allows shorter preambles, reducing implementation loss.
  - Increases the forward error correction (FEC) T-byte size to 16 bytes per Reed Solomon block (T=16) with programmable interleaving.

Note Cisco IOS Release 12.2(15)BC2 does not support the Synchronous Code Division Multiple Access (S-CDMA) modulation technique that is also specified in the DOCSIS 2.0 specification.

Modes of Operation

Depending on the configuration, the DOCSIS 2.0 A-TDMA Service feature supports either DOCSIS or Euro-DOCSIS operation:

- DOCSIS cable networks are based on the ITU J.83 Annex B physical layer standard and Data-over-Cable Service Interface Specifications (DOCSIS, Annex B) specification, which use 6 MHz National Television Systems Committee (NTSC) channel plans. In this mode, the downstream uses a 6 MHz channel width in the 85 to 860 MHz frequency range, and the upstream supports multiple channel widths in the 5 to 42 MHz frequency range.

  Cisco IOS Release 12.2(15)BC2 also supports an extended frequency range for DOCSIS cable networks, in which the upstream channel widths can range from 5 to 55 MHz.
- EuroDOCSIS cable networks are based on the ITU J.112 Annex A physical layer standard and European DOCSIS (EuroDOCSIS, Annex A) specification, which use 8 MHz Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) channel plans. In this mode, the downstream uses an 8 MHz channel width in the 85 to 860 MHz frequency range, and the upstream supports multiple channel widths in the 5 to 65 MHz frequency range.

Note The difference between DOCSIS and EuroDOCSIS is at the physical layer. To support a DOCSIS or EuroDOCSIS network requires the correct configuration of the DOCSIS 2.0 A-TDMA Service card, as well as upconverters, diplex filters, and other equipment that supports the network type.

When using Cisco IOS Release 12.2(15)BC2, the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards support all DOCSIS 1.1-specified and all DOCSIS 2.0-specified A-TDMA radio frequency (RF) data rates, channel widths, and modulation schemes.

The table below shows the maximum supported DOCSIS 1.1 data rates.

Table 16: Maximum DOCSIS 1.1 Data Rates

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

The table below shows the maximum supported DOCSIS 2.0 (A-TDMA-mode) data rates.

Table 17: Maximum DOCSIS 2.0 (A-TDMA-mode) Data Rates

Upstream Channel Width	Modulation Scheme	Baud Rate Sym/sec	Maximum Raw Bit Rate Mbit/sec
6.4 MHz	64-QAM 32-QAM 16-QAM 8-QAM QPSK	5.12 M	30.72 25.60 20.48 15.36 10.24
3.2 MHz	64-QAM 32-QAM 16-QAM 8-QAM QPSK	2.56 M	15.36 12.80 10.24 7.68 5.12

Upstream Channel Width	Modulation Scheme	Baud Rate Sym/sec	Maximum Raw Bit Rate Mbit/sec
1.6 MHz	64-QAM	1.28 M	7.68
	32-QAM		6.40
	16-QAM		5.12
	8-QAM		3.84
	QPSK		2.56
800 kHz	64-QAM	640 K	3.84
	32-QAM		3.20
	16-QAM		2.56
	8-QAM		1.92
	QPSK		1.28
400 kHz	64-QAM	320 K	1.92
	32-QAM		1.60
	16-QAM		1.28
	8-QAM		0.96
	QPSK		0.64
200 kHz	64-QAM	160 K	0.96
	32-QAM		0.80
	16-QAM		0.64
	8-QAM		0.48
	QPSK		0.32

Modulation Profiles

To simplify the administration of A-TDMA and mixed TDMA/A-TDMA modulation profiles, the DOCSIS 2.0 A-TDMA Service feature provides a number of preconfigured modulation profiles that are optimized for different modulation schemes. We recommend using these preconfigured profiles.

Each mode of operation also defines a default modulation profile that is automatically used when a profile is not specifically assigned to an upstream. These default modulation profiles (1, 21, 41, 101, 121, 141, 201, 221, and 241, depending on the cable interface line cards that are installed) cannot be deleted. The valid range for modulation profiles depends on the cable interface being used and the type of modulation profile being created. The table below lists the valid ranges according to cable interface and modulation type:

Table 18: Allowable Ranges for Modulation Profiles

Cable Interface	DOCSIS 1.X (TDMA)	Mixed DOCSIS 1.X/2.0	DOCSIS 2.0 (A-TDMA)
Cisco uBR7100 series	1 to 10 (default is 1)	N/A	N/A
Cisco uBR-MC16C	1 to 10 (default is 1)	N/A	N/A
Cisco uBR-MC16S	1 to 10 (default is 1)	N/A	N/A
Cisco uBR-MC28C	1 to 10 (default is 1)	N/A	N/A
Cisco uBR-MC5X20S/U	21 to 30 (default is 21)	121 to 130 (default is 121)	221 to 230 (default is 221)
Cisco uBR-MC16U/X, Cisco uBR-MC28U/X	41 to 50 (default is 41)	141 to 150 (default is 141)	241 to 250 (default is 241)

Benefits

The DOCSIS 2.0 A-TDMA Service feature provides the following benefits to cable service providers and their partners and customers:

- Full compatibility with DOCSIS 1.0 and DOCSIS 1.1 cable modems (CMs) and cable modem termination systems (CMTS).
- Additional channel capacity in the form of more digital bits of throughput capacity in the upstream path.
- Increased protection against electronic impairments that occur in cable systems, allowing for a more robust operating environment.

How to Configure DOCSIS 2.0 A-TDMA Services

This section contains the following:

Creating Modulation Profiles

This section describes how to create modulation profiles for the different modes of DOCSIS operations, using the preconfigured modulation profile options.

Creating a TDMA Modulation Profile

This section describes how to create a modulation profile for the DOCSIS 1.0/DOCSIS 1.1 TDMA mode of operation, using one of the preconfigured modulation profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk** | **robust-mix**} **Example:** `Router(config)# cable modulation-profile 3 mix` `Router(config)# cable modulation-profile 4 qpsk`	Creates a preconfigured modulation profile, where the burst parameters are set to their default values for each burst type: • *profile*— Specifies the modulation profile number. The valid range depends on the cable interface line card: ◦ For the Cisco uBR-MC5X20S/U card, the valid range is 21 to 30. The system creates profile 21 as a default TDMA-only modulation profile. ◦ For the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X card, the valid range is 41 to 50. The system creates profile 41 as a default TDMA-only modulation profile. ◦ For all other cable interface line cards, the valid range is 1 to 10. The system creates profile 1 as a default TDMA-only modulation profile. • The following preconfigured profiles are available: ◦ **mix—** Default QPSK/16-QAM profile. ◦ **qam-16—** Default 16-QAM profile. ◦ **qpsk—** Default QPSK profile. ◦ **robust-mix—** Default QPSK/16-QAM profile that is more robust and more able to deal with noise than the mix profile. **Note** You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating a Mixed Mode Modulation Profile

This section describes how to create a modulation profile for the mixed TDMA/A-TDMA mode of operation, using one of the preconfigured modulation profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* {**mix-high** | **mix-low** | **mix-mid** | **mix-qam** | **qam-16** | **qpsk** | **robust-mix-high** | **robust-mix-mid** | **robust-mix-qam**} **Example:** `Router(config)# cable modulation-profile 143 mix-medium` `Router(config)# cable modulation-profile 144 mix-high`	Creates a preconfigured modulation profile, where the burst parameters are set to their default values for each burst type: • *profile*— Specifies the modulation profile number. The valid range depends on the cable interface line card: ◦ For the Cisco uBR-MC5X20S/U card, the valid range is 121 to 130. The system creates profile 121 as a default mixed mode modulation profile. ◦ For the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards, the valid range is 141 to 150. The system creates profile 141 as a default mixed mode modulation profile. • The following preconfigured profiles are available: ◦ **mix-high** and **robust-mix-high—**Default QPSK/64-QAM profile. ◦ **mix-low—**Default QPSK/16-QAM profile. ◦ **mix-mid** and **robust-mix-mid—** Default QPSK/32-QAM profile. ◦ **mix-qam** and **robust-mix-qam—** Default 16-QAM/64-QAM profile. ◦ **qam-16—** Default 16-QAM modulation profile. ◦ **qpsk—** Default QPSK modulation profile. **Note** The **robust-mix** profiles are similar to but more robust than the **mix** profiles, so that they more able to detail with noise on the upstream. **Note** You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating an A-TDMA Modulation Profile

This section describes how to create a modulation profile for the DOCSIS 2.0 A-TDMA mode of operation, using one of the preconfigured modulation profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* {**mix-high** | **mix-low** | **mix-mid** | **mix-qam** | **qam-8** | **qam-16** | **qam-32** | **qam-64** | **qpsk** | **robust-mix-high** | **robust-mix-low** | **robust-mix-mid**} **Example:** `Router(config)# cable modulation-profile 242 qam-32` `Router(config)# cable modulation-profile 243 qam-64`	Creates a preconfigured modulation profile, where the burst parameters are set to their default values for each burst type: • *profile*— Specifies the modulation profile number. The valid range depends on the cable interface line card: ◦ For the Cisco uBR-MC5X20S/U card, the valid range is 221 to 230. The system creates profile 221 as a default DOCSIS 2.0 A-TDMA mode modulation profile. ◦ For the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards, the valid range is 241 to 250. The system creates profile 241 as a default DOCSIS 2.0 A-TDMA mode modulation profile. • The following preconfigured profiles are available: ◦ **mix-high** and **robust-mix-high—** Default QPSK/64-QAM profile. ◦ **mix-low** and **robust-mix-low—** Default QPSK/16-QAM profile. ◦ **mix-mid** and **robust-mix-mid—** Default QPSK/32-QAM profile. ◦ **mix-qam—** Default 16-QAM/64-QAM profile. ◦ **qam-8—** Default 8-QAM profile.

	Command or Action	Purpose
		◦ **qam-16—** Default 16-QAM profile. ◦ **qam-32—** Default 32-QAM profile. ◦ **qam-64—** Default 64-QAM profile. ◦ **qpsk—** Default QPSK modulation profile. **Note** The **robust-mix** profiles are similar to but more robust than the **mix** profiles, so that they more able to detail with noise on the upstream. **Note** You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the DOCSIS Mode and Profile on an Upstream

This section describes how to configure an upstream for a DOCSIS mode of operation, and then to assign a particular modulation profile to that upstream.

Note By default, all upstreams are configured for ATDMA-only mode, using the default modulation profile of 1, 21, or 41, depending on the cable interface line card.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface cable** *x/y/z* **Example:** `Router(config)# interface cable c5/1/1`	Enters interface configuration mode for the indicated cable downstream interface.
Step 4	**cable upstream** *n* **docsis-mode** {**atdma** | **tdma** | **tdma-atdma**} **Example:** `Router(config-if)# cable upstream 0 docsis-mode atdma` `Router(config-if)# cable upstream 1 docsis-mode tdma-atdma`	Configures the upstream for the desired DOCSIS mode of operation: • *n*— Specifies the upstream port. Valid values start with 0 for the first upstream port on the cable interface line card. • **atdma**— Configures the upstream for DOCSIS 2.0 A-TDMA modulation profiles only (default). • **tdma**— Configures the upstream for DOCSIS 1.X TDMA modulation profiles only. • **tdma-atdma**— Configures the upstream for both A-TDMA and TDMA operation (mixed mode).
Step 5	**cable upstream** *n* **modulation-profile** *profile* [*profile2*] **Example:** `Router(config-if)# cable upstream 0 modulation-profile 241` `Router(config-if)# cable upstream 1 modulation-profile 131`	Assigns the particular modulation profile to this upstream. • *n*— Specifies the upstream port. Valid values start with 0 for the first upstream port on the cable interface line card. • *profile*— Specifies the modulation profile to be used on this upstream. The valid range for the *profile* parameter depends on the current DOCSIS mode: ◦ If the upstream is configured for DOCSIS 1.0 and DOCSIS 1.1 mode, the valid range is 21 to 30 for the Cisco uBR-MC5X20S, and 41 to 50 for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X. The valid range is 1 to 10 for all other cards. ◦ If the upstream is configured for DOCSIS 1.X and DOCSIS 2.0 mixed mode, the valid range is 121 to 130 for the Cisco uBR-MC5X20S, and 141 to 150 for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X. ◦ If the upstream is configured for DOCSIS 2.0 A-TDMA mode, the valid range is 221 to 230 for the Cisco uBR-MC5X20S, and 241 to 250 for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X. • *profile2*— (Optional) Specifies the number of a secondary modulation profile that the interface uses when noise on the upstream increases to the point that the primary modulation profile can no longer be used. (The secondary profile should specify a more robust profile, in terms of coping with noise, than the primary profile.) **Note** The type of modulation profiles must match the DOCSIS mode configured for the upstream, using the **cable upstream docsis-mode** command.

	Command or Action	Purpose
Step 6	**cable upstream** *n* **equalization-coefficient** **Example:** `Router(config-if)# cable upstream 0 equalization-coefficient`	(Optional) Enables the use of a DOCSIS pre-equalization coefficient on an upstream. • *n*— Upstream port. Valid values start with 0 for the first upstream port on the cable interface line card.
Step 7	**cable upstream** *n* **ingress-noise-cancellation** *interval* **Example:** `Router(config-if)# cable upstream 0 ingress-noise-cancellation 400`	(Optional) Configures how often, in milliseconds, the line card should sample the signal on an upstream to correct any ingress noise that has appeared on that upstream. • *n*— Upstream port. Valid values start with 0 for the first upstream port on the cable interface line card. • *interval*— Sample interval. Valid range is 10 to 3000 milliseconds, with a default value of 200 milliseconds.
Step 8	**cable upstream** *n* **maintain-psd** **Example:** `Router(config-if)# cable upstream 0 maintain-psd`	(Optional) Requires DOCSIS 2.0 cable modems that are operating on an ATDMA-only upstream to maintain a constant power spectral density (PSD) after a modulation rate change. • *n*— Upstream port. Valid values start with 0 for the first upstream port on the cable interface line card. **Note** Repeat Step 3, on page 297 through Step 8, on page 298 for each cable interface and upstream to be configured.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring the DOCSIS 2.0 A-TDMA Services

This section contains the following:

Displaying Modulation Profiles

To display the modulation profiles that are currently defined on the CMTS, use the **show cable modulation-profile** command without any options:

```
Router# show cable modulation-profile

Mod IUC     Type  Preamb Diff FEC    FEC   Scrambl Max  Guard Last Scrambl Preamb
                  length enco T      k     seed    B    time  CW          offset
                                BYTES  BYTES         size size  short
21  request qpsk  64     no   0x0    0x10  0x152   0    8     no   yes     0
21  initial qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
21  station qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
```

```
21  short   qpsk  72     no   0x5    0x4B  0x152   6    8     yes  yes     0
21  long    qpsk  80     no   0x8    0xDC  0x152   0    8     yes  yes     0
121 request qpsk  64     no   0x0    0x10  0x152   0    8     no   yes     0
121 initial qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
121 station qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
121 short   qpsk  72     no   0x5    0x4B  0x152   6    8     yes  yes     0
121 long    qpsk  80     no   0x8    0xDC  0x152   0    8     yes  yes     0
121 a-short 64qam 128    no   0x5    0x63  0x152   10   8     yes  yes     0
121 a-long  64qam 128    no   0xF    0xC8  0x152   0    8     yes  yes     0
221 request qpsk  64     no   0x0    0x10  0x152   0    8     no   yes     0
221 initial qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
221 station qpsk  128    no   0x5    0x22  0x152   0    48    no   yes     0
221 short   qpsk  72     no   0x5    0x4B  0x152   6    8     yes  yes     0
221 long    qpsk  80     no   0x8    0xDC  0x152   0    8     yes  yes     0
221 a-short 64qam 128    no   0x5    0x63  0x152   10   8     yes  yes     0
221 a-long  64qam 128    no   0xF    0xC8  0x152   0    8     yes  yes     0
Router#
```

To display a specific modulation profile in detail, specify the profile number with the **show cable modulation-profile** command:

```
Router# show cable modulation-profile 221

Mod IUC     Type  Pre Diff FEC  FEC  Scrmb Max Guard Last Scrmb Pre   Pre   RS
                  len enco T    k    seed  B   time  CW         offst Type
                            BYTE BYTE       siz size  short
221 request qpsk  68  no   0x0  0x10 0x152 0   8     no   yes   0     qpsk0 no
221 initial qpsk  2   no   0x0  0x10 0x0   0   0     no   no    0     qpsk1 no
221 station qpsk  128 no   0x5  0x22 0x152 0   48    no   yes   0     qpsk0 no
221 a-short 32qam 160 no   0x9  0x4C 0x152 6   8     yes  yes   0     qpsk1 no
221 a-long  64qam 132 no   0xC  0xE7 0x152 0   8     yes  yes   0     qpsk1 no
221 a-ugs   16qam 80  no   0x3  0xE7 0x152 0   8     yes  yes   0     qpsk1 no
Router#
```

Displaying Cable Modem Capabilities and Provisioning

To display the capabilities of the online cable modems and how the modems were provisioned, use the **show cable modem mac** command:

```
Router# show cable modem mac

MAC Address    MAC          Prim  Ver    Prov    Frag Concat PHS Priv  DS    US
               State        Sid                                       Saids Sids
0007.0e03.69a1 online       2     DOC1.1 DOC1.1  yes  yes    yes BPI+  0     4
0007.0e03.6a05 online       3     DOC1.1 DOC1.1  yes  yes    yes BPI+  0     4
0007.0e03.6981 online       4     DOC1.1 DOC1.1  yes  yes    yes BPI+  0     4
0007.0e03.69e9 online       2     DOC1.1 DOC1.1  yes  yes    yes BPI+  0     4
0090.963e.d312 online(pt)   4     DOC1.1 DOC1.0  no   yes    yes BPI   8     4
0008.0e06.7a90 online(pt)   56    DOC1.0 DOC1.0  no   yes    no  BPI   0     0
0002.8a0e.a392 online(pt)   57    DOC1.0 DOC1.0  no   no     no  BPI   0     0
0000.39e8.9a4e online(pt)   58    DOC1.0 DOC1.0  no   yes    no  BPI   0     0
0000.39ac.4e57 online       151   DOC2.0 DOC1.0  no   yes    no  BPI   0     0
0090.963e.d314 online(pt)   152   DOC1.1 DOC1.0  no   yes    yes BPI   8     4
0008.0e06.7ab8 online(pt)   153   DOC2.0 DOC1.0  no   yes    no  BPI   0     0
0007.0e03.6cf5 online(pt)   154   DOC1.0 DOC1.0  no   yes    no  BPI   0     0
0007.0e03.69f1 online       155   DOC1.1 DOC1.0  no   yes    yes BPI+  0     4
0007.0e03.6855 online       156   DOC1.1 DOC1.0  no   yes    yes BPI+  0     4
0007.0e03.6ca1 online       157   DOC1.1 DOC1.0  no   yes    yes BPI+  0     4
0050.daf8.0296 online(pt)   158   DOC1.0 DOC1.0  no   no     no  BPI   0     0
0002.8a0e.a38c online(pt)   159   DOC2.0 DOC2.0  no   no     no  BPI   0     0
Router#
```

To display how many cable modems of each DOCSIS type are online each upstream, use the **show cable modem mac summary** command:

```
Router# show cable modem mac summary
```

```
                                Cable Modem Summary
                                -------------------
                           Mac Version                    Provision Mode
Interface       Total   DOC2.0   DOC1.1   DOC1.0   Reg/Online   DOC 2.0   DOC1.1   DOC1.0
Cable3/0/U1     1       0        1        0        1            0         1        0
Cable3/0/U2     1       0        1        0        1            0         1        0
Cable3/0/U3     1       0        1        0        1            0         1        0
Cable3/1/U0     1       0        1        0        1            0         0        1
Cable3/1/U1     1       0        0        1        1            0         0        1
Cable3/1/U2     3       0        1        2        3            0         1        2
Cable6/0/U1     9       1        5        3        9            1         0        8
Cable6/0/U2     1       0        1        0        1            0         0        1
Cable6/0/U2     2       2        0        0        2            2         0        0
Router#
```

Configuration Examples for DOCSIS 2.0 A-TDMA services

This section contains the following:

Creating Modulation Profiles Examples

This section contains the following:

Example: DOCSIS 1.0/DOCSIS 1.1 TDMA Modulation Profiles

The following sample configurations show typical modulation profiles for the DOCSIS 1.0/DOCSIS 1.1 TDMA mode of operation when using the Cisco uBR-MC5X20S/U cable interface line card:

- Profile 1 is the default profile for TDMA operations that is automatically created on the router for legacy cable interface line cards.
- Profile 21 is the default profile for TDMA operations that is automatically created on the router for the Cisco uBR-MC5X20S/U card.
- Profiles 24 and 25 use the preconfigured 16-QAM and QPSK modulation profiles.
- Profile 26 is a typical QPSK modulation profile using some customized burst parameters.

```
cable modulation-profile 1 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 1 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 short 4 76 12 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 1 long 9 236 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 24 qam-16
cable modulation-profile 25 qpsk
cable modulation-profile 26 request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed
cable modulation-profile 26 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 26 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 26 short 4 76 12 8 qpsk scrambler 152 no-diff 80 shortened
cable modulation-profile 26 long 8 236 0 8 qpsk scrambler 152 no-diff 80 shortened
```

Example: Mixed TDMA/A-TDMA Modulation Profiles

The following sample configurations show typical modulation profiles for the DOCSIS 1.X/DOCSIS 2.0 mixed TDMA/A-TDMA mode of operation:

- Profile 121 is the default profile for mixed mode operations that is automatically created on the router for the Cisco uBR-MC5X20S/U card.
- Profiles 122 through 126 use the preconfigured mixed mode modulation profiles.
- Profile 127 is a typical mixed mode modulation profile some customized burst parameters.

```
cable modulation-profile 121 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 121 initial 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed uw16
cable modulation-profile 121 station 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed uw16
cable modulation-profile 121 short 5 75 6 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 121 long 8 220 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 121 a-short qpsk0 0 18 5 99 10 8 64qam scrambler 152 no-diff 128
shortened uw8
cable modulation-profile 121 a-long qpsk0 0 18 15 200 0 8 64qam scrambler 152 no-diff 128
shortened uw8
cable modulation-profile 122 mix-high
cable modulation-profile 123 mix-low
cable modulation-profile 124 mix-medium
cable modulation-profile 125 qam-16
cable modulation-profile 126 qpsk
cable modulation-profile 127 request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed
cable modulation-profile 127 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 127 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 127 short 6 76 7 8 16qam scrambler 152 no-diff 160 shortened
cable modulation-profile 127 long 8 231 0 8 16qam scrambler 152 no-diff 160 shortened
cable modulation-profile 127 a-short 9 76 6 8 32qam scrambler 152 no-diff 160 shortened
qpsk1 1 2048
cable modulation-profile 127 a-long 12 231 0 8 64qam scrambler 152 no-diff 132 shortened
qpsk1 1 2048
```

Example: DOCSIS 2.0 A-TDMA Modulation Profiles

The following sample configurations show typical modulation profiles for the DOCSIS 2.0 A-TDMA mode of operation:

- Profile 221 is the default profile for A-TDMA mode operations.
- Profiles 222 through 226 use the preconfigured A-TDMA mode modulation profiles.
- Profile 227 is a typical A-TDMA mode modulation profile customized burst parameters.

```
cable modulation-profile 221 request qpsk0 0 0 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed
 uw8
cable modulation-profile 221 initial qpsk0 0 0 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
 uw16
cable modulation-profile 221 station qpsk0 0 0 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
 uw16
cable modulation-profile 221 short qpsk0 0 0 5 75 6 8 qpsk scrambler 152 no-diff 72 shortened
 uw8
cable modulation-profile 221 long qpsk0 0 0 8 220 0 8 qpsk scrambler 152 no-diff 80 shortened
 uw8
cable modulation-profile 221 a-short qpsk0 0 18 5 99 10 8 64qam scrambler 152 no-diff 128
shortened uw8
cable modulation-profile 221 a-long qpsk0 0 18 15 200 0 8 64qam scrambler 152 no-diff 128
shortened uw8

cable modulation-profile 222 qam-8
cable modulation-profile 223 qam-16
cable modulation-profile 224 qam-32
cable modulation-profile 225 qam-64
cable modulation-profile 226 qpsk

cable modulation-profile 227 request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed qpsk0 1
2048
cable modulation-profile 227 initial 0 16 0 0 qpsk no-scrambler no-diff 2 fixed qpsk1 0 18
```

```
cable modulation-profile 227 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed qpsk0
1 2048
cable modulation-profile 227 a-short 9 76 6 8 32qam scrambler 152 no-diff 160 shortened
qpsk1 1 2048
cable modulation-profile 227 a-long 12 231 0 8 64qam scrambler 152 no-diff 132 shortened
qpsk1 1 2048
cable modulation-profile 227 a-ugs 3 231 0 8 16qam scrambler 152 no-diff 80 shortened qpsk1
 1 2048
```

Assigning Modulation Profiles to Upstreams Examples

This section contains the following:

Example: Assigning DOCSIS 1.0/DOCSIS 1.1 TDMA Modulation Profiles

The following sample configuration shows DOCSIS 1.0/DOCSIS 1.1 TDMA modulation profiles being assigned to the upstreams on two cable interfaces on the Cisco uBR-MC5X20S/U cable interface line card. The TDMA modulation profile (profile 21) is assigned to the upstreams on cable interface 5/1/0, and modulation profile 22 is assigned to the upstreams on cable interface 5/1/1.

Note Starting with Cisco IOS Release 12.2(33)SCG, the **cable upstream docsis-mode atdma** command is the default configuration for upstreams, so this command is not shown in these sample configurations.

```
interface Cable5/1/0
 ip address 22.0.0.1 255.0.0.0
 ip helper-address 10.10.0.4
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 2
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable upstream 4 channel-width 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 21
 cable upstream 4 shutdown
 cable upstream 5 channel-width 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 21
 cable upstream 5 shutdown
!
interface Cable5/1/1
 ip address 21.0.0.1 255.0.0.0
 ip helper-address 10.10.0.4
 cable downstream annex B
```

```
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 2
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 22
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 22
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 22
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 22
 cable upstream 3 shutdown
```

Example: Assigning Mixed TDMA/A-TDMA Modulation Profiles

The following sample configuration shows mixed mode TDMA/A-TDMA modulation profiles being assigned to the upstreams on a cable interface on the Cisco uBR-MC5X20S/U cable interface line card. All upstreams are configured for mixed mode and profile 121 is assigned to them, but only the first upstream is enabled.

```
interface Cable5/1/2
 ip address 21.0.0.1 255.0.0.0
 ip helper-address 10.10.0.4
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 2
 cable upstream 0 frequency 30000000
 cable upstream 0 docsis-mode tdma-atdma
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 121
 no cable upstream 0 shutdown
 cable upstream 1 docsis-mode tdma-atdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 121
 cable upstream 1 shutdown
 cable upstream 2 docsis-mode tdma-atdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 121
 cable upstream 2 shutdown
 cable upstream 3 docsis-mode tdma-atdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 121
 cable upstream 3 shutdown
```

Example: Assigning DOCSIS 2.0 A-TDMA Modulation Profiles

The following sample configuration shows DOCSIS 2.0 A-TDMA modulation profiles being assigned to the upstreams on two cable interfaces on the Cisco uBR-MC5X20S/U cable interface line card. Only the first upstream on cable interface c7/1/1 is enabled for A-TDMA mode and assigned an A-TDMA profile. The first

three upstreams on cable interface c7/1/2 are enabled for A-TDMA mode, and they are using the default A-TDMA modulation profile of 221.

```
interface Cable7/1/1
 ip address 20.0.0.1 255.0.0.0
 ip helper-address 10.10.0.4
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 frequency 30000000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 minislot-size 1
 cable upstream 0 modulation-profile 221
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 41
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 41
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 41
 cable upstream 3 shutdown
!
interface Cable7/1/2
 ip address 71.2.1.1 255.255.255.0 secondary
 ip address 71.72.71.1 255.255.255.0
 load-interval 30
 no keepalive
 cable map-advance static
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 cable downstream channel-id 2
 no cable downstream rf-shutdown
 cable upstream 0 frequency 30000000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 power-level 0
 no cable upstream 0 concatenation
 no cable upstream 0 fragmentation
 cable upstream 0 modulation-profile 221
 no cable upstream 0 shutdown
 cable upstream 1 frequency 5104000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 power-level 6
 cable upstream 1 channel-width 200000
 cable upstream 1 minislot-size 32
 cable upstream 1 modulation-profile 221
 cable upstream 1 shutdown
 cable upstream 2 frequency 38800000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 800000
 cable upstream 2 minislot-size 32
 cable upstream 2 modulation-profile 221
 cable upstream 2 shutdown
 cable upstream 3 docsis-mode atdma
 cable upstream 3 frequency 14000000
 cable upstream 3 power-level -6
 cable upstream 3 channel-width 400000
 cable upstream 3 minislot-size 32
 cable upstream 3 modulation-profile 221
 cable upstream 3 shutdown
```

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Configuring the Cisco uBR-MC16U/X Card	*Configuring the Cisco uBR-MC16U/MC16X Cable Interface Line Card* , at the following URL: http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr16u_x/configuration/guide/mc16uxfm.html
Configuring the Cisco uBR-MC28U/X Card	*Configuring the Cisco uBR-MC28U/MC28X Cable Interface Line Card* , at the following URL: http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr28u_x/configuration/guide/mc28uxfm.html

Standards

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

MIBs

MIBs	MIBs Link
• DOCS-BPI-PLUS-MIB • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-CABLE-DEVICE-TRAP-MIB • DOCS-IF-EXT-MIB • DOCS-IF-MIB (RFC 2670) • DOCS-QOS-MIB • DOCS-SUBMGT-MIB • IGMP-STD-MIB (RFC 2933)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers

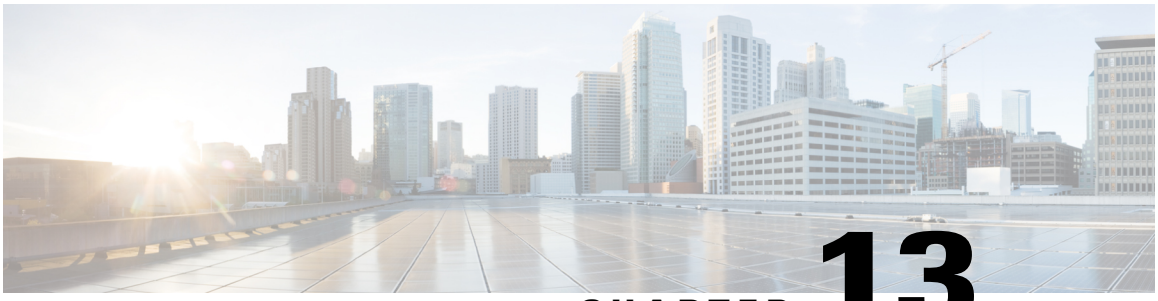
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 19: Feature Information for DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers	12.2(15)CX	This feature was introduced for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards on the Cisco uBR7246VXR router. The following commands are new or modified: • **cable modulation-profile** • **cable upstream channel-width** • **cable upstream docsis-mode** • **cable upstream equalization-coefficient** • **cable upstream maintain-psd** • **cable upstream minislot-size** • **cable upstream modulation-profile** • **show cable modulation-profile** • **show interface cable mac-schedule** • **show cable modem verbose** • **show cable modem phy** • **show controllers cable**
DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers	12.2(15)BC2	This feature was supported on the Cisco uBR-MC5X20S/U cable interface line cards on the Cisco uBR10012 router.

Feature Name	Releases	Feature Information
DOCSIS 2.0 A-TDMA Modulation Profiles for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 13

DOCSIS 3.0 Downstream Bonding for Bronze Certification

First Published: December 17, 2008

Last Updated: November 29, 2010

The DOCSIS 3.0 Downstream Bonding for Bronze Certification feature helps cable operators offer new, more bandwidth-intensive services by adding one or more additional downstream quadrature amplitude modulation (QAM) channels to the standard broadband DOCSIS system.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS 3.0 Downstream Bonding for Bronze Certification

The table below shows the hardware compatibility prerequisites for the DOCSIS 3.0 Downstream Bonding for the Bronze Certification feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 20: Cable Hardware Compatibility Matrix for Downstream Bonding

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [15]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [16]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

15 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
16 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for DOCSIS 3.0 Downstream Bonding for Bronze Certification

- Although verbose receive channel profile (RCP) reporting can be enabled on a given cable interface, this does not eliminate the need to define a receive channel configuration (RCC) template to support a non-standard RCP ID.
- An RCC template configuration cannot be modified or removed if it is associated to any MAC domain. The operator must remove the association first to make modifications to an existing RCC template.
- The CMTS does not create a new RCP or modify an existing RCP based on the verbose RCP report from a cable modem at run time. The operator should explicitly add an RCC template and the RCP ID association per RCP requirements.

Information About DOCSIS 3.0 Downstream Bonding for Bronze Certification

The DOCSIS 3.0 Downstream Bonding for Bronze Certification enables high-speed broadband access and helps cable operators offer more bandwidth-intensive services by adding one or more additional downstream quadrature amplitude modulation (QAM) channels to the standard broadband DOCSIS system. This new set of downstream channels is grouped into one larger channel, known as a bonded channel.

Channel bonding combines several RF channels into one virtual channel. Data rates in this virtual channel range from hundreds of megabits to potentially gigabits per second, creating more available bandwidth in the network.

Receive Channel Profile

An RCP is an encoding that represents the receive channels and receive modules of a cable modem. A cable modem communicates to the CMTS one or more RCP encodings within its registration request using either verbose description, which contains complete subtype encoding defined in DOCSIS 3.0, or simple description, which only contains RCP identifiers.

The cable modem reporting method is controlled by the CMTS using a MAC Domain Descriptor (MDD).

Receive Channel Configuration

A cable modem reports its ability to receive multiple channels with one or more RCP encodings in a REG-REQ or REG-REQ-MP message. Each receive channel profile describes a logical representation of the cable modem's downstream physical layer in terms of receive channels (RCs) and receive modules (RMs). The CMTS initially configures the cable modem's receive channels and receive modules with an RCC encoding in the registration response.

Beginning Cisco IOS Release 12.2(33)SCB, this feature supports any arbitrary RCP ID configuration and receive channel configuration on a Cisco uBR10012 universal broadband router and Cisco IOS Release 12.2(33)SCD provides this support on the Cisco uBR7225VXR and Cisco uBR7246VXR routers.

RCC Template

You can configure one or more RCC templates for an RCP. An RCC template configures the physical layer components described by an RCP, including receive modules and receive channels to specific downstream frequencies. The template also specifies the interconnections among receive modules, or between a receive module and a receive channel. An RCC template can be associated only to the cable interface (MAC domain).

Channel Assignment

The CMTS assigns a receive channel configuration encoding to a DOCSIS 3.0-certified cable modem operating in a Multiple Receive Channel (MRC) mode during cable modem registration.

Prior to Cisco IOS Release 12.2(33)SCB, the channel assignment was based on a random selection from eligible bonding groups.

With the implementation of this feature, the DOCSIS 3.0-certified cable modem reports its receiving capabilities and characteristics using the receive channel profile type, length, value (TLV) list in the registration request message. Based on this report, the CMTS assigns an RCC encoding that is compatible with the reported RCP.

Cable modems operating in an MRC mode are assigned an RCC encoding that is derived from an RCC template, which is associated with an RCP.

An RCC encoding can also be derived from a wideband interface configuration if an RCC template is not configured and associated to the MAC domain of a particular cable modem.

Note The cable modem can support up to 8 physical downstream channels. If you do not have 8 channel bonding group configured, the modem can lock a downstream primary channel and then decide to either use the bonding group that primary is part of or use the other 4-channel bonding group, which makes it appear as 5 downstream channels.
In the following example you can see the CMTS or cable modem add the 5th downstream channel when you use two wideband interfaces with 4 DS channels.

```
Downstream Channel DCID RF Channel : 40 1/2/0:16
Downstream Channel DCID RF Channel : 28 1/2/0:4
Downstream Channel DCID RF Channel : 29 1/2/0:5
Downstream Channel DCID RF Channel : 30 1/2/0:6
Downstream Channel DCID RF Channel : 31 1/2/0:7
```

Downstream Traffic Forwarding

DOCSIS 3.0 introduces the concept of assigning downstream service flows of cable modems, which are operating in an MRC mode, to downstream (DS) channels or bonding groups. Forwarding interfaces assigned to service flows (SFs) can be either DS channel interfaces (cable, integrated cable interfaces or modular cable interfaces) or downstream bonding groups (wideband interfaces).

These forwarding interfaces will override the default CMTS assignment of a service flow to a wideband interface.

Note Valid interfaces that are available for SF assignment must be a subset of the cable modem's assigned RCC encoding.

Service Flow Priority in Downstream Extended Header

The purpose of the feature is to be able to reflect the traffic priority of downstream packets into the DOCSIS extended header. The priority is derived from the service flow that the packet is mapped to. Priority refers to the service flow priority specified in the CM configuration file, or the Cisco CMTS service class configuration.

The service flow priority can be set using cable modem configuration file, or dynamic configuration.

By default, this feature is disabled on Cisco cBR-8 router, user can use **cable service flow priority** command to enable this feature.

How to Configure RCC Encoding

The following tasks describe how to configure a receive channel configuration encoding for a receive channel profile:

Configuring an RCC Template

You must configure an RCC template with a unique RCP ID for a particular CMTS. A valid RCC template consists of a configured RCP ID, RMs, and RCs.

Before You Begin

To configure an RCC template, the verbose encoding of the corresponding RCP ID must be available.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rcc-template** *index* **Example:** `Router(config)# cable rcc-template 1`	Defines an RCC template. • *index* —Specifies an RCC template ID in the range 1 to 255.

Configuring RCC Encoding

You can configure an RCC encoding after defining an RCC template. The CMTS derives an RCC or RCCs from the RCC template for each MAC Domain Downstream Service Group (MD-DS-SG). Each RCC encoding contains all operational DS channels with their channel parameters, including the frequency match RC attribute specified in the RCC template. An RCC template specifies the intended receive channel assignment in the available DS spectrum.

The following information is required for RCC configuration:

- The RCC templates associated to the MAC domain
- DS channel physical parameters including frequency and connected-receive-module index
- DS channel primary capable indicator
- DS channel membership to the MD-DS-SG
- Cable modem membership to the MD-DS-SG

Note If an RCC template is removed from a MAC domain through configuration, the CMTS removes all of the RCC encodings derived from the RCC template, and all cable modems assigned to the RCC encodings are marked offline.

Before You Begin

At least one RC must be configured as a primary RC.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rcc-template** *index* **Example:** `Router(config)# cable rcc-template 1`	Defines the RCC template. • *index* —Specifies an RCC template ID in the range 1 to 255.
Step 4	**rcp-id** *rcp-id* **Example:** `Router(config-rcc-template)# rcp-id 00 10 00 00 03`	• *rcp-id*—Specifies an RCP ID for the RCC template. The valid range is 00 00 00 00 00 to FF FF FF FF. By default the RCP ID is set to 00 00 00 00 00.

	Command or Action	Purpose
Step 5	**receive-module** *index* **first-channel-center-frequency** *Hz* [**connected-receive-module** *index*] **Example:** `Router(config-rcc-template)# receive-module 1 first-channel-center-frequency 555000000 connected-receive-module 1`	Specifies a receive module configuration for the selected RCP. • *index*—Specifies the index value for the receive module. The valid range is 1 to 10. • **first-channel-center-frequency**—Specifies the center frequency of the first channel of the receive module channel block. The first channel center frequency assignment defines a frequency within the minimum and maximum range of center frequencies configured for the RM. • *Hz*—Specifies the center frequency value in Hz. The valid range is from 55000000 to 1050000000. • **connected-receive-module**—(Optional) Specifies a nested receive module in the RCC template. Generally, only one receive module is configured for an RCC template. • *index*—(Optional) Specifies the index value for the connected receive module. The valid range is from 1 to 10.
Step 6	**receive-channel** *index* **center-frequency** *Hz* **connected-receive-module** *index* [**primary**] **Example:** `Router(config-rcc-template)# receive-channel 1 center-frequency 555000000 connected-receive-module 1 primary`	Specifies a receive channel configuration for the selected RCP. • *index*—Specifies the index value for the receive channel. The valid range is from 1 to 10. • **center-frequency**—Specifies the center frequency for the receive channel. • *Hz*—Specifies the center frequency value in Hz. The valid range is from 55000000 to 1050000000. • **connected-receive-module**—Specifies a nested receive module in the RCC template. Generally, only one receive module is configured for an RCC template. • *index*—Specifies the index value for the connected receive module. The valid range is from 1 to 10. • **Primary**—(Optional) Indicates that it is a primary channel and an RCC can be derived from this channel. At least one receive-channel must be configured as primary.

What to Do Next

After defining an RCC template, you must assign the template to a cable interface. See Assigning an RCC Template to a Cable Interface , on page 316.

Assigning an RCC Template to a Cable Interface

This section describes how to assign an RCC template to a cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/port* | *slot*/*subslot/port*} **Example:** `Router(config)# interface cable7/0/0`	Specifies the cable interface line card on a Cisco CMTS router: • *slot*—Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface).
Step 4	**cable rcc-template** *index* **Example:** `Router(config-if)# cable rcc-template 1`	Assigns the RCC template to the specified cable interface. • *index*—Specifies the template you want to assign to the cable interface. The valid range is from 1 to 255.

Verifying the RCC Configuration

To verify the runtime RCCs on a cable interface, use the **show cable mac-domain rcc** command as shown in the following example:

Cisco uBR10012 Router

```
Router# show cable mac-domain c8/0/0 rcc
```

```
RCC-ID   RCP                RCs MD-DS-SG CMs   WB/RCC-TMPL
1        00 00 00 00 00     2   0        0     WB (101)
2        00 10 00 00 03     3   2        0     RCC-TMPL (1)
```

Cisco uBR7200 Series Routers

```
Router# show cable mac-domain cable 5/0 rcc
RCC-ID   RCP                RCs MD-DS-SG CMs   WB/RCC-TMPL
1        00 00 00 00 00     3   0        3     WB (25)
```

The table below shows descriptions for the fields displayed by this command.

Table 21: show cable mac-domain rcc Field Descriptions

Field	Description
RCC-ID	RCC index per MAC domain.
RCP	The receive channel profile associated with the RCC object.
RCs	Total number of DS channels.
MD-DS-SG	Indicates the MAC domain DS service group for which the RCC is configured.
CM	Total number of cable modems associated with the RCC object.
WB/RCC-TMPL	Indicates the wideband interface or the RCC template.

Note A zero (0) value in the RCP or MD-DS-SG field indicates that the RCC encoding is configured directly through a wideband interface configuration and not through any RCC templates.

Verifying the MD-DS-SG Configuration

To verify the MD-DS-SG on a cable interface, use the **show cable mac-domain downstream-service-group** command as shown in the following example:

```
Router# show cable mac-domain cable 5/0 downstream-service-group
Cable    MD-DS-SG             RF
IF       Id        Resource   Chan     Primary Chan
C5/0     1         5/0        00-03    0
```

How to Configure Attribute Masks

DOCSIS 3.0 introduces the concept of assigning service flows to channels or bonding groups based on binary attributes. The attribute masks configured on a cable, modular, integrated or wideband interface are called provisioned attribute masks.

The two types of attributes are as follows:

- Specification-defined attributes—Contain default values based on the characteristics of the channel or bonding group.
- Operator-defined attributes—Default to zero.

The operator can configure a provisioned attribute mask for each channel and provisioned bonding group to assign values to the operator-defined binary attributes. The operator can also assign new values to override the default values of the specification-defined attributes.

The operator can configure a required attribute mask and a forbidden attribute mask for a service flow in the cable modem configuration file. These required and forbidden attribute masks are optionally provided on the DOCSIS 3.0 service flows and are matched with the provisioned attribute masks of the interfaces.

Each service flow is optionally configured with the following TLV parameters:

- Service flow required attribute mask—To configure this, assign a service flow to a channel that has a 1-bit in all positions of its provisioned attribute mask corresponding to the 1-bit in the service flow required attribute mask.
- Service flow forbidden attribute mask—To configure this, assign a service flow to a channel that has a 0-bit in all positions of its provisioned attribute mask corresponding to the 1-bit in the service flow forbidden attribute mask.

Additionally, in a cable modem-initiated dynamic service request, the cable modem can include a required attribute mask and a forbidden attribute mask for a service flow. The CMTS assigns service flows to channels or bonding groups so that all required attributes are present and no forbidden attributes are present in the cable modem configuration file.

The table below lists the supported binary attributes for channels and bonding groups.

Table 22: Binary Attributes

Bit Position	Definition
Bit 0	Bonded—This bit is zero for all individual channel interfaces and one for all bonding groups.
Bit 1	Low latency—This bit is set when the interface can provide relatively low latency service. This bit is set to zero for all channels, and left up to the operator to define.
Bit 2	High availability—This bit is set to zero for all channels, and left up to the operator to define.
Bit 3:15	Reserved—Set to zero.

Bit Position	Definition
Bit 16:31	Operator defined—Set to zero by default.

You can configure provisioned attribute masks for cable, integrated cable, wideband cable, and modular cable interfaces.

Prerequisites

- To assign an interface to a wideband cable modem's service flow, the interface must be a subset of the cable modem's RCC.
- To assign a service flow to a modular shared port adapter (SPA) channel, the corresponding modular cable interface must be configured and operational.
- To assign a service flow to an integrated cable (IC) channel, the corresponding integrated cable interface must be configured and operational.

Restrictions

- The dynamic bonding group is not supported.
- The service flow from a narrowband cable modem is always assigned to the primary interface of the cable modem. No attribute checking is performed in this case.

This section describes the following:

Configuring Provisioned Attributes for a Cable Interface

The default provisioned attribute is zero for a cable interface.

Note Provisioning the cable downstream attribute-mask command is not supported on the Cisco uBR7225VXR and Cisco uBR7246VXR routers.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port*	Specifies the cable interface line card on a Cisco CMTS router:

	Command or Action	Purpose
	Example: `Router(config)# interface cable 7/0/0`	• *slot*—Chassis slot number of the cable interface line card. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface).
Step 4	**cable downstream attribute-mask** *mask* **Example:** `Router(config-if)# cable downstream attribute-mask 800000ff`	Specifies the mask for the interface.

Configuring Provisioned Attributes for a Modular Cable Interface

This section describes how to configure the provisioned attributes for a modular cable interface on the Cisco uBR10012 universal broadband router. The default provisioned attribute is zero for a modular cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface modular-cable** *slot/bay/port:nb-channel-number* **Example:** `Router(config)# interface modular-cable 1/0/1:5`	Specifies the modular cable interface and enters interface configuration mode. • *slot*—The slot where a SIP resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for SIPs. • *bay*—The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). • *port*—Specifies the interface number on the SPA. • *nb-channel-number*—Specifies the narrowband channel number.

	Command or Action	Purpose
Step 4	**cable attribute-mask** *mask* **Example:** `Router(config-if)# cable attribute-mask 800000ff`	Specifies the mask for the modular-cable interface.

Configuring Provisioned Attributes for an Integrated Cable Interface

The default provisioned attribute is zero for an integrated cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface integrated-cable** {*slot/port* | *slot/subslot/port*}*:rf-channel* **Example:** `Router(config)# interface integrated-cable 1/0/0:0`	Specifies the cable interface line card on a Cisco CMTS router: • *slot*—Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *rf-channel*—RF channel number with a range of 0 to 3.

	Command or Action	Purpose
Step 4	**cable attribute-mask** *mask* **Example:** `Router(config-if)# cable attribute-mask 800000ff`	Specifies the mask for the interface.

Configuring Provisioned Attributes for a Wideband Cable Interface

The default provisioned attribute is 0x80000000 for a wideband cable interface, and the zero bit is automatically added to the wideband cable interface whenever an attribute is configured for that interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** {*slot/port* | *slot/subslot/port*}:*wideband-channel* **Example:** `Router(config)# interface wideband-cable 1/0/1:4`	Specifies the wideband cable interface and enters interface configuration mode:
Step 4	**cable downstream attribute-mask** *mask* **Example:** `Router(config-if)# cable downstream attribute-mask 800000ff`	Specifies the mask for the interface.

Verifying the Attribute-Based Service Flow Assignments

To verify the attribute-based assignment of service flows on a cable interface, use the **show interface cable service-flow** or **show interface wideband-cable service-flow** command as shown in the following example:

```
Router# show interface cable 3/0 service-flow

Sfid  Sid   Mac Address     QoS  Param Index Type  Dir  Curr  Active  DS-ForwIf/
                           Prov Adm   Act             State Time    US-BG/CH
```

```
17    4     001c.ea37.9aac  3    3     3     P     US   act   13h21m  CH 3
18    N/A   001c.ea37.9aac  4    4     4     P     DS   act   13h21m  Wi3/0:0
21    6     001c.ea37.9b5a  3    3     3     P     US   act   13h21m  CH 4
22    N/A   001c.ea37.9b5a  4    4     4     P     DS   act   13h21m  Wi3/0:0
23    7     0016.925e.654c  3    3     3     P     US   act   13h21m  CH 3
24    N/A   0016.925e.654c  4    4     4     P     DS   act   13h21m  In3/0:0

Router# show interface wideband-cable 5/1:0 service-flow
Sfid  Sid   Mac Address     QoS Param Index Type  Dir Curr   Active  DS-ForwIf/
                           Prov  Adm  Act           State  Time    US-BG/CH
3     8193  ffff.ffff.ffff   3     3    3   S(s)  DS  act    2h06m   Wi5/1:0
```

The table below shows descriptions for the fields displayed by this command:

Table 23: show interface cable service-flow Field Descriptions

Field	Description
Sfid	Identifies the service flow identification number. **Note** Primary service flow IDs are displayed even for offline cable modems because they are needed for modem re-registration.
Sid	Identifies the service identification number (upstream service flows only).
Mac Address	Identifies the MAC address for the cable modem.
QoS Parameter Index Prov	Identifies the QoS parameter index for the provisioned state of this flow.
QoS Parameter Index Adm	Identifies the QoS parameter index for the Admitted state of this flow.
QoS Parameter Index Act	Identifies the QoS parameter index for the Active state of this flow.
Type	Indicates if the service flow is the primary flow or a secondary service flow. Secondary service flows are identified by an “S” (created statically at the time of registration, using the DOCSIS configuration file) or “D” (created dynamically by the exchange of dynamic service messages between the cable modem and CMTS).
Dir	Indicates if this service flow is DS or US.
Curr State	Indicates the current run-time state of the service flow.
Active Time	Indicates the length of time this service flow has been active.
DS-ForwIf/US-BG/CH BG/DS	Indicates the bonding group ID or the downstream RFID of the forwarding interface assigned to the downstream service flow.

How to Enable Service Flow Priority in Downstream Extender Header

The following tasks describe how to enable service flow priority in downstream extender header:

Enabling Service Flow Priority in Downstream Extender Header

This section describes how to enable service flow priority in downstream extender header on the Cisco cBR-8 routers:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service flow priority** **Example:** `Router(config)# cable service flow priority`	Enables the service flow priority in downstream extender header.

Verifying the Enablement of the Service Flow Priority in Downstream Extended Header

To verify the enablement of the service flow priority in downstream extended header, use the **show running-config | in service flow** or **show cable modem** [*ip-address* | *mac-address*] **verbose** command as shown in the following example:

```
Router# show running-config | in service flow
cable service flow priority

Router# show cable modem 100.1.2.110 verbose

MAC Address                     : 0025.2e2d.74f8
IP Address                      : 100.1.2.110
IPv6 Address                    : 2001:420:3800:909:7964:98F3:7760:ED2
Dual IP                         : Y
Prim Sid                        : 1
Host Interface                  : C3/0/0/U0
MD-DS-SG / MD-US-SG             : N/A / N/A
MD-CM-SG                        : 0x900000
Primary Downstream              : In3/0/0:32 (RfId : 12320, SC-QAM)
Wideband Capable                : Y
DS Tuner Capability             : 8
RCP Index                       : 6
```

```
RCP ID                              : 00 00 00 00 00
Downstream Channel DCID RF Channel : 191   3/0/0:32 (SC-QAM)
UDC Enabled                         : N
US Frequency Range Capability       : Standard (5-42 MHz)
Extended Upstream Transmit Power    : 0dB
Multi-Transmit Channel Mode         : N
Upstream Channel                    : US0
Ranging Status                      : sta
Upstream SNR (dB)                   : 39.8
Upstream Data SNR (dB)              : 36.12
Received Power (dBmV)               : -1.00
Timing Offset              (97.6 ns): 1799
Initial Timing Offset               : 1799
Rng Timing Adj Moving Avg(0.381 ns): 0
Rng Timing Adj Lt Moving Avg        : 0
Rng Timing Adj Minimum              : 0
Rng Timing Adj Maximum              : 0
Pre-EQ Good                         : 0
Pre-EQ Scaled                       : 0
Pre-EQ Impulse                      : 0
Pre-EQ Direct Loads                 : 0
Good Codewords rx                   : 8468
Corrected Codewords rx              : 0
Uncorrectable Codewords rx          : 0
Phy Operating Mode                  : atdma
sysDescr                            :
Downstream Power                    : 0.00 dBmV (SNR = ----- dB)
MAC Version                         : DOC3.0
QoS Provisioned Mode                : DOC1.1
Enable DOCSIS2.0 Mode               : Y
Service Flow Priority               : N
Modem Status                        : {Modem= online, Security=disabled}
Capabilities                        : {Frag=Y, Concat=Y, PHS=Y}
Security Capabilities               : {Priv=, EAE=N, Key_len=}
L2VPN Capabilities                  : {L2VPN=N, eSAFE=N}
L2VPN type                          : {CLI=N, DOCSIS=N}
Sid/Said Limit                      : {Max US Sids=16, Max DS Saids=15}
Optional Filtering Support          : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support          : {Taps/Symbol= 1, Num of Taps= 24}
CM Capability Reject               : {15,22,23,24,25,26,27,28,29,35,36,38}
Flaps                               : 3(Oct 8  16:22:23)
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 0 aborts, 2 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 294 packets, 25903 bytes
Total US Throughput                 : 143 bits/sec, 0 packets/sec
Total DS Data                       : 91 packets, 10374 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
LB group ID assigned                : 1
LB group ID in config file          : N/A
LB policy ID                        : 0
LB policy ID in config file         : 0
LB priority                         : 0
Tag                                 : d30
Required DS Attribute Mask          : 0x0
Forbidden DS Attribute Mask         : 0x0
Required US Attribute Mask          : 0x0
Forbidden US Attribute Mask         : 0x0
Service Type ID                     :
Service Type ID in config file      :
Active Classifiers                  : 0 (Max = NO LIMIT)
CM Upstream Filter Group            : 0
CM Downstream Filter Group          : 0
CPE Upstream Filter Group           : 0
CPE Downstream Filter Group         : 0
DSA/DSX messages                    : permit all
Voice Enabled                       : NO
DS Change Times                     : 0
Boolean Services                    : 0
CM Energy Management Capable        : N
CM Enable Energy Management         : N
CM Enter Energy Management          : NO
```

```
Battery Mode                        : N
Battery Mode Status                 :
Number of Multicast DSIDs Support   : 16
MDF Capability Mode                 : 2
IGMP/MLD Version                    : MLDv2
FCType10 Forwarding Support         : Y
Features Bitmask                    : 0x0
Total Time Online                   : 6h00m   (6h00m    since last counter reset)
CM Initialization Reason            : POWER_ON
```

Enabling Verbose Reporting for Receive Channel Profiles

A receive channel profile is an encoding that represents the receive channels and receive modules of a cable modem. A cable modem communicates to the CMTS one or more RCP encodings within its registration request using either verbose description, which contains complete subtype encodings defined in DOCSIS 3.0, or simple description, which only contains RCP identifiers.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/port* | *slot*/*subslot/port*} **Example:** `Router(config)# interface cable7/0/0`	Specifies the cable interface line card on a Cisco CMTS router: • *slot*—Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface).
Step 4	**cable rcp-control verbose** **Example:** `Router(config-if)# cable rcp-control verbose`	Enables RCP reporting with verbose description.

Configuration Example for an RCC Template

The following sample shows an RCC template configuration:

```
...
!
cable rcc-template 1
  rcp-id 00 10 00 00 03
  receive-module 1 first-center-frequency 555000000 connected-receive-module 1
  receive-channel 1 center-frequency 555000000 connected-receive-module 1 primary
  receive-channel 2 center-frequency 561000000 connected-receive-module 1
  receive-channel 3 center-frequency 567000000 connected-receive-module 1
!
...
!
interface Cable5/1
 downstream Integrated-Cable 5/1 rf-channel 0 upstream 0-3
 cable rcc-template 1
 cable rcp-control verbose
...
```

Additional References

The following sections provide references related to the DOCSIS 3.0 Downstream Bonding for Bronze Certification feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband routers)	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco DOCSIS 3.0 Downstream Solution	*Cisco DOCSIS 3.0 Downstream Solution Design and Implementation Guide* http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_2.0/ds_solu.html
DOCSIS 3.0 Downstream Channel Bonding	*Cisco Cable Wideband Solution Design and Implementation Guide* http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_1.0/wb_solu.html

Standards and RFCs

Standard	Title
CM-SP-MULPIv3.0-I08-080522	MAC and Upper Layer Protocols Interface Specifications

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DOCSIS 3.0 Downstream Bonding for Bronze Certification

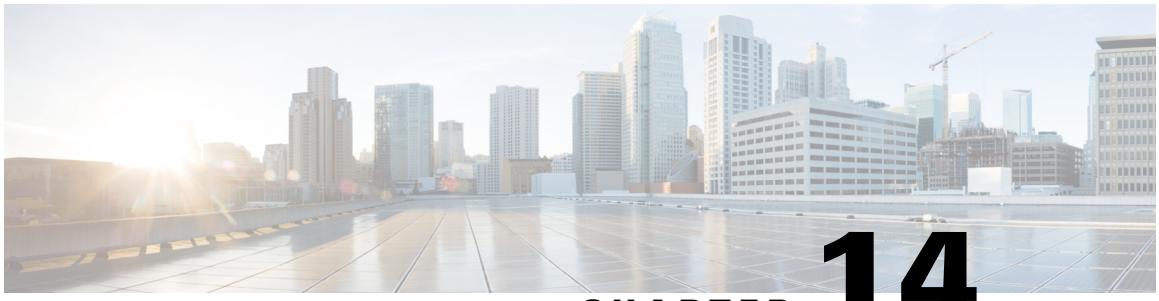
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 24: Feature Information for DOCSIS 3.0 Downstream Bonding for Bronze Certification

Feature Name	Releases	Feature Information
DOCSIS 3.0 Downstream Bonding for Bronze Certification	12.2(33)SCB	This feature was introduced to meet the Bronze requirements for the DOCSIS 3.0 downstream bonding. It also includes receive channel configuration for receive channel profiles. In Cisco IOS Release 12.2(33)SCB, this feature was introduced on the Cisco uBR10012 router. The following sections provide information about this feature: • How to Configure RCC Encoding, on page 313 • How to Configure Attribute Masks, on page 318 • Enabling Verbose Reporting for Receive Channel Profiles, on page 326 The following commands were introduced or modified in this release: • **cable rcc-template** • **cable rcp-control verbose** • **rcp-id** • **receive-module** • **receive-channel** • **show cable mac-domain rcc** • **show interface cable service-flow** • **show cable modem**

Feature Name	Releases	Feature Information
DOCSIS 3.0 Downstream Bonding for Bronze Certification	12.2(33)SCD	In Cisco IOS Release 12.2(33)SCD, this feature was introduced on the Cisco uBR7225VXR and Cisco uBR7246VXR routers. The following commands were introduced or modified: • **interface cable** • **show cable mac-domain rcc** • **show cable mac-domain downstream-service-group**



CHAPTER 14

Downstream Channel ID Assignment on the Cisco CMTS Routers

First Published: November 29, 2010

The DOCSIS downstream channel ID (DCID) is defined as an 8-bit identifier for recognizing a Downstream Channel within a MAC Domain. All CMTS downstream channels are assigned a DCID by default that may be subsequently changed by configuration. It is used in most DOCSIS downstream packet headers and its valid range is from 1 to 255 (0 is reserved for network management purposes).

Note All downstream channels in a MAC domain must have a unique DCID within the MAC domain.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Downstream Channel ID Assignment on the Cisco CMTS Routers

The table below shows the hardware compatibility matrix for this feature.

Note The hardware components introduced in a particular Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 25: Downstream Channel ID Assignment - Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [17]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [18]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V 2

17 The Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.
18 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2, and not with NPE-G1.

Information About Downstream Channel ID Assignment on the Cisco CMTS Routers

These are the downstream channel ID assignment features in the Cisco IOS Release 12.2(33)SCB and later releases:

- DCID uniqueness is provided by keeping the wideband SPA DCID range unique compared to the MAC domain host card range.
- Unique DCIDs are provided for all channels within controllers, such as the wideband SPA bay controller, Cisco uBR-MC2020V controller, Cisco uBR-MC88V controller, and Cisco uBR-MC3GX60V controller.

Note All DCIDs for all controllers on a card need not be unique, since channels from multiple controllers are most likely parts of different fiber nodes. DCIDs need to be unique only for default downstream channel ID assignments. With automatic Channel ID assignment, channel IDs may repeat within a controller depending on the fiber node configuration.

- Redundancy schemes are allowed where downstream channels from different cable interface line cards are bound to the same fiber node. If one card fails, cable modems are able to lock to a frequency on a channel from the other line card. Since DCID uniqueness is enforced for channels in a fibre node, channels from both line cards should have unique DCIDs.
- ID assignment for the Cisco uBR7225 universal broadband router with a line card in slot 1 begins at DCID 1 on slot 1 and for the Cisco uBR7246 universal broadband router, which begins with cable line card slots at slot 3, the ID assignment begins with DCID 1 on slot 3. A Cisco uBR10012 router begins assigning IDs with channel 1 at slot 5 and SPA slots follow as described in Table 26: Downstream Channel ID Per Subslot Scheme , on page 334.

Note You can configure the DCIDs manually to suit your plant floor layout requirements.

- In the Cisco uBR-MC3GX60V cable line card where the channel count on the router is 576, with eight Cisco uBR-MC3GX60V line cards, or even greater if the router also includes Wideband SPAs, there is no slot-based default channel ID scheme that would avoid potential channel ID conflicts.

  The Manual DCID scheme was introduced in the Cisco IOS Release 12.2(33)SCB1 and the automatic DCID that includes the Cisco uBR-MC3GX60V line card, was introduced in Cisco IOS Release 12.2(33)SCE.

Manual Downstream Channel ID Assignment on the Cisco CMTS Routers

For the Cisco uBR10-MC5x20 cable interface line card, the manual downstream channel ID is configured on the cable interface. For controller-based line cards, such as Cisco Wideband SPA, Cisco UBR-MC20X20V,

Cisco uBR-MC88V and Cisco uBR-MC3GX60V, the manual downstream channel ID is configured in the controller per RF channel.

The tables below describe the DCID scheme per subslot:

Table 26: Downstream Channel ID Per Subslot Scheme

	8/1	8/0	7/1	7/0	6/1	6/0	5/1	5/0	slot 3	slot 1
SPA Bay 0									217-240	193-216
SPA Bay 1									217-240	193-216
SPA Bay 2									217-240	193-216
SPA Bay 3									217-240	193-216
uBR-MC520 DS/0	169	145	121	97	73	49	25	1		
uBR-MC520 DS/1	173	149	125	101	77	53	29	5		
uBR-MC520 DS/2	177	153	129	105	81	57	33	9		
uBR-MC520 DS/3	181	157	133	109	85	61	37	13		
uBR-MC520 DS/4	185	161	137	113	89	65	41	7		
uBR-MC2020V	169-188	145-164	121-140	97-116	73-92	49-68	25-44	1-20		
uBR-MC3GX60V controller 0	73-96	1-24	73-96	1-24	73-96	1-24	73-96	1-24		
uBR-MC3GX60V controller 1	97-120	25-48	97-120	25-48	97-120	25-48	97-120	25-48		
uBR-MC3GX60V controller 2	121-144	49-72	121-144	49-72	121-144	49-72	121-144	49-72		

Table 27: Downstream Channel ID Per Subslot Scheme - Cisco IOS Release 12.3(23)BCx

	8/1	8/0	7/1	7/0	6/1	6/0	5/1	5/0	slot 3	slot 1
SPA Bay 0									24- 47	24-47
SPA Bay 1									48-71	48-71

	8/1	8/0	7/1	7/0	6/1	6/0	5/1	5/0	slot 3	slot 1
uBR-MC520	188-192	180-184	168-172	160-164	148-152	140-144	128-132	120-124		

Automatic Downstream Channel ID Assignment on the Cisco CMTS Routers

Starting with Cisco IOS Release 12.2(33)SCE, it is possible to automatically assign a unique set of downstream channel IDs to meet all DOCSIS requirements. However, DCIDs are assigned automatically at the fiber node, therefore only those deployments that use fiber node configuration can use automatic DCID assignment.

DCID is computed automatically as channels are added to the fiber nodes.

Note Automatic DCID assignment is not supported on the Cisco uBR7225 and Cisco uBR7246 universal broadband routers.

Service Impact

Changing the DOCSIS downstream channel ID causes cable modems to re-register. Cable modems receive MAC Domain Descriptor (MDD) and Upstream Channel Descriptor (UCD) messages with a changed DCID in their headers.

- Enabling the automatic DCID assignment displays the following message:

```
WARNING: Enabling automatic DCID assignment will cause modems to flap and will apply
to all fiber nodes on this CMTS.
```

- Disabling the automatic DCID assignment displays the following message:

```
WARNING: Disabling automatic DCID assignment will no longer enforce channel-id uniqueness
 at fiber nodes. Channel ID changes may require manual verification to prevent conflicts.
```

- If there is a DCID conflict with another channel in the MAC Domain, the following error message is displayed:

```
ERROR: <slot>/<subslot>/<controller> rf-channel <channel>: The downstream channel id
conflicts with interface Mo<slot>/<subslot>/<controller>:channel. Downstream channel
id must be unique in a CGD.
```

- After automatic DCID assignment is configured, if there is a DCID conflict when a downstream channel that belongs to a fiber node is added to a MAC Domain, the automatic DCID feature tries to resolve the conflict by assigning another automatic DCID and the following message is displayed:

```
WARNING: The downstream channel id conflict for <slot>/<subslot>/<controller> rf-channel
 <channel> was resolved by Automatic DCID Assignment.
Please run "interface <md-slot>/<md-subslot>/<md-index>" followed by
"<slot>/<subslot>/<controller> rf-channel <channel>" again in order to add the channel.
```

To add the channel, use this channel grouping domain (CGD) command again:

cable downstream *x/y/z* **rf-channel** *channel*

Note The resolved DCIDs may conflict with the other existing channels in the MAC Domain.

- If automatic DCID is configured and the channel does not belong to a fiber node, or if automatic DCID cannot resolve the conflict, the following message is displayed:

```
WARNING: The downstream channel id conflict for <slot>/<subslot>/<controller> rf-channel
 <channel> could not be resolved by Automatic DCID Assignment.
```

To resolve this issue, add the channel to a fiber node.

How to Configure Downstream Channel ID Assignment on the Cisco CMTS Routers

The following sections describe how to configure downstream channel ID assignment.

Configuring Manual Downstream Channel ID Assignment

Restriction

- Shared bonding groups on the Cisco uBR-MC2020V do not require DCID user-renumbering intervention. However, SPA-based shared bonding groups may require renumbering using the range from 241 to 255. Shared bonding groups on the Cisco uBR-MC3GX60V require DCID user-renumbering if the shared bonding group and the modems data bonding group are on the same line card.
- The DCID for a channel on a working line card must be carried forward to the channel on the protect line card upon failover. The opposite is true for revert.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router(config)# interface cable 6/0/1`	Enters interface configuration mode for the Channel Grouping Domain host line card.

	Command or Action	Purpose
Step 4	**cable downstream-channel-id** *id* **Example:** `Router(config-if)# cable downstream channel-id 44`	Configures the downstream channel ID.

Configuring Automatic Downstream Channel ID Assignment

Automatic DCID assignment should be permanently configured. However, if you need to remove the feature, use the **no** or **default** commands.

Note The **no** or **default** form of the command is not written to startup-config file.

In this case, the DCIDs are retained as computed for all channels, and are not set to the defaults of the channels. Save the configuration containing the newly-assigned DCIDs to the startup-config file by using the **write memory** command.

When you enable automatic DCID assignment, any DCID conflict arising due to adding a channel in a fiber-node is resolved automatically.

Restriction

- After running the **cable downstream-channel-id automatic** command in the configuration, manually editing the configuration file in an editor to add RF channels to the fiber nodes could cause DCID conflicts. The feature assumes all channels in fiber nodes have unique automatic DCIDs in global configuration mode. If the configuration is manually edited and the feature does not verify the unique DCIDs, the DCIDs of the newly-added channels may conflict with those of the existing channels. To fix any DCID conflicts, undo and re-apply the global automatic DCID configuration.

  Note Re-applying global automatic DCID configuration is a disruptive operation.

  To avoid DCID conflicts, edit the configuration to configure the fiber nodes, then run the **cable downstream-channel-id automatic** command so all channels have unique automatic DCIDs.

  Make additions to the fiber nodes on the Cisco uBR10012 router command line interface with the automatic DCID configured.

- The **cable downstream-channel-id automatic** command can be configured only on the Cisco uBR10012 universal broadband router.
- The **cable downstream-channel-id automatic** command should not be manually edited in to the startup-config file, since it does not guarantee unique DCIDs for channels in the fiber node.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable downstream-channel-id automatic** **Example:** `Router(config)# cable downstream-channel-id automatic`	Specifies automatic assignment of the DCIDs by the Cisco CMTS.

Example

This example displays the restriction on manually editing configurations:

```
Router# show run | include automatic
cable downstream-channel-id automatic

Router# show cable fiber-node 3
------------------------------------------------------------------------------
Fiber-Node 3
Channel(s) : downstream Modular-Cable 1/1/0: 0
Channel ID(s): 3
Channel : downstream Cable 6/1/0
Channel ID : 1
upstream Cable 6/1: 0-3
FN Config Status: Configured (status flags = 0x01)
MDD Status: Valid
router#
```

If you manually edit the startup-config file in an editor to add a downstream channel, for example, 5/0/0 rf-channel 0, from a newly-added line card, 5/0, it causes a conflict.

```
Router> configure terminal
Router# cable fiber-node 3
Router# downstream Modular-Cable 5/0/0 rf-channel 0
```

If this downstream channel is added on the Cisco uBR10012 router, the automatic DCID assignment feature automatically resolves it. However, since the startup-config file was manually edited to add the downstream channel, the automatic DCID assignment feature is unable to resolve it. This causes a DCID conflict when the edited startup-config file is loaded on the Cisco uBR10012 router and invalidates the fiber node.

```
down Modular-Cable 5/0/0 rf-channel 0
Fiber node 3 is invalid for:
DS frequency is not unique.
DS channel id is not unique.
Warning: D3.0 CMs cannot get w-online with an invalid fiber-node.
router#
```

What to Do Next

Run the **show cable fibernode** command to view DCIDs assigned to all the channels in the fiber node.

```
Router# show cable fiber-node 5
Fiber-Node         Config Status
Fiber-Node 5
    Description: Interface c5/0/4
    Channels                          DOCSIS Channel-IDs
 ------------------------------------------------------
       Modular-Cable 3/3/0:  1-3      2,3,4
       Cable 5/0/4      1
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
```

Additional References

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco IOS CMTS Cable Command Reference, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Downstream Channel ID Assignment on the Cisco CMTS Routers

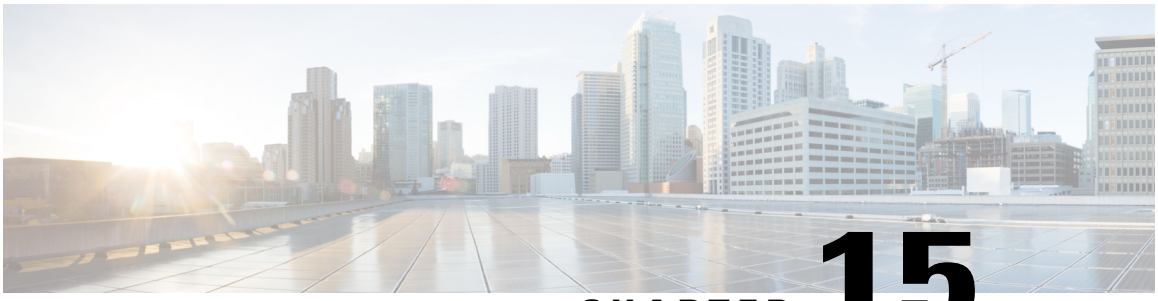
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 28: Feature Information for Downstream Channel ID Assignment on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Downstream Channel ID Assignment on the Cisco CMTS Routers	12.2(33)SCE	This feature was introduced.



CHAPTER 15

Downstream Resiliency Bonding Group

First Published: July 2012

With more wideband (WB) modems being deployed in cable plants, WB modem resiliency is an important feature. The Wideband Modem Resiliency feature works well when a large number of WB modems experience an RF impairment. However, if a comparatively smaller number of cable modems (CMs) observe an impairment on an RF channel, then all CMs using that RF channel are shut down irrespective of whether they are affected or not. Instead, the solution should be to communicate with the affected CMs using the good RF channel, without affecting the other CMs.

In the Wideband Modem Resiliency feature, CMs with multiple impaired RF channels are moved to a single primary RF channel. Because the CMs are moved to a narrowband (NB) interface, this scenario may cause performance issues.

Starting with Cisco IOS Release 12.2(33)SCG, the Downstream Resiliency Bonding Group feature allows CMs with multiple impaired RF channels to be allocated to a dynamically-created wideband interface, which ensures that the performance of the wideband CMs is not drastically affected.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Downstream Resiliency Bonding Group

- Set aside WB interfaces so that new WB interfaces can be dynamically created from the reserved list of WB interfaces.
- Free up RF bandwidth so that those RF channels can be added to a resiliency bonding group (RBG).
- Remove all existing RBG configuration from the WB interface.

Table 29: Downstream Resiliency Bonding Group – Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCG and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCG and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V • Cisco UBR-MC3GX60V[19]
Cisco uBR7246VXR Universal Broadband Router[20]	Cisco IOS Release 12.2(33)SCG and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCG and later releases • Cisco uBR-MC88V
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCG and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCG and later releases • Cisco uBR-MC88V

19 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

20 This feature is supported on the Cisco uBR7246VXR and Cisco uBR7225VXR routers only in Cisco IOS Release 12.2(33)SCG1 and later releases.

Restrictions for the Downstream Resiliency Bonding Group

- If an existing wideband interface is reserved as a Resiliency Bonding Group (RBG) and later the RBG is removed (through the **no cable ds-resiliency** command), the modems using this RBG go offline and the RBG configuration itself is deleted. Therefore, it is highly recommended that users should not configure an existing BG as an RBG.

- This feature is enabled only when the number of cable modems observing an RF channel impairment is *below* the resiliency threshold. If the number of cable modems on an impaired RF channel is above the resiliency threshold, the impaired RF channel is temporarily removed from the bonding group.
- In Cisco IOS Release 12.2(33)SCG, a CM is assigned to an RBG on a first-come-first-served basis. To handle this feature optimally, it is recommended to set aside more WB interfaces and RF channel bandwidth.
- The Cisco CMTS controls the freeing of unused RBGs, when there is no modem using the RGB. The freeing of the unused RGB may take some time and the RGB, which is not completely free cannot be used by the modems. Irrespective of the number of configured RBGs, if all the old RBGs are not completely set free and if the Cisco CMTS tries to move the cable modem to a new RBG, the Cisco CMTS moves the cable modem to the primary DS channel instead of RBG.
- Only SFs on the WB interface associated with the primary SF are moved to an RBG. SFs on other interfaces will not be moved.
- Static SFs are assigned to an RBG on a best effort quality of service (QoS).
- If the **resiliency rf-change-trigger** setting does not have the **secondary** keyword set, only the primary SF is moved to the RBG or a NB interface.
- If the Downstream Resiliency Bonding Group feature is not enabled to use an RBG, only cable modems with impairments on the primary WB interface are moved to the NB interface.
- SFs carrying multicast traffic are not moved.
- The Cisco CMTS prevents configuration changes on a protect line card. Therefore, RBGs are not added or removed on a protect line card. Impaired SFs are moved only to a WB, NB, or existing RBGs on the protect line card.
- When the WB interface is in standby mode and after a line card switchover, if a cable modem experiences an RF channel impairment, and after impairment if there are no preexisting RBG that matches the new set of channels, in such case, the Cisco CMTS does not create a new Downstream Resiliency Bonding Group and channels are not assigned to it and the cable modem is moved to a Narrow Band state.

There may not be enough reserved bonding groups to support all modems facing an impairment at any given time thus the following restrictions must be considered:

- Each RBG has at least two RF channels.
- RBG RF assignments are always a subset of the RF channel assignment of the parent WB interface.
- If an RBG is unavailable for a cable modem, the SF of the CM is moved to a NB interface.
- If a high percentage of cable modems experience an RF impairment and there are no more available bonding group IDs, the impaired RF itself may be removed from the bonding group. Removal of an impaired RF from a parent bonding group is also reflected in the RBG. If an RBG drops to a single RF, all SFs are moved to the NB interface.

The Downstream Resiliency Bonding Group feature has the following cross-functional restrictions:

- Dynamic service flows that require a committed information rate (CIR), typically voice flows, are created on the NB interface when an RF channel is impaired. Because all SFs assigned to an RBG are best effort only, voice calls may report a quality issue.
- Cable modems participating in the resiliency mode do not take part in load balancing.

- The Downstream Resiliency Bonding Group feature is only supported in the Dynamic Bandwidth Sharing (DBS) mode.

Information About Downstream Resiliency Bonding Group

In releases earlier than Cisco IOS Release 12.2 (33)SCG, bonding groups were static and created manually from the command line interface. The Cisco CMTS utilized the unused bonding groups for the Wideband Modem Resiliency feature.

However, starting with Cisco IOS Release 12.2 (33)SCG, you can set aside unused bonding groups as RBGs. Ensure that each RF channel is assigned at least 1% of the available bandwidth. Use the **cable rf-channel bandwidth-percent** command to configure the RF channel bandwidth.

Note If the bandwidth-percent is set to 100, the Cisco CMTS does not add any RFs to the RBG. In other words, this feature will not be enabled.

The Cisco CMTS controls the assignment and freeing of unused RBGs. If an RF channel is removed from a WB interface, it is also removed from any associated RBGs.

Note If the wideband interface is in standby mode, the Cisco CMTS does not assign or free up the unused downstream bonding group.

A suspended RF channel is restored for all affected wideband interfaces when a specified number of cable modems report (via CM-STATUS) that the channel connectivity is restored. The Wideband Modem Resiliency feature defines the specified number of cable modems as half of the configured count or percentage of rf-change-trigger, or both. For example, if the count is 20 and the percent is 10, then the number of cable modems reporting recovery should reduce the count to 10 and the percent to 5 for the suspended RF channel to be restored.

Finding a Best-Fit RBG for the Cable Modem

A bonding group is a list of channels that provide a means to identify the channels that are bonded together. The Cisco CMTS assigns a service flow (SF) to an RBG based on the attributes of the SF and the attributes of the individual channels of the bonding group.

In the Downstream Resiliency Bonding Group feature, when a line card receives a CM-STATUS message from the cable modem informing the line card that there is an RF channel impairment, the line card checks for the number of good RF channels and:

- Moves the cable modem to narrowband mode if there is only one available RF channel.
- Moves the cable modem to wideband mode if the cable modem reports all RF channels are in good state.
- Moves the cable modem to an RBG if there are two or more good RF channels, with at least one RF channel impaired, and if the Downstream Resiliency Bonding Group feature is enabled.

When the Cisco CMTS receives a message from the line card to move a cable modem to an RBG, the Cisco CMTS attempts to find an existing RBG or creates an RBG that satisfies the impairment.

Note If two or more RBGs are reserved for the same wideband controller, the Cisco CMTS creates one RBG for each cable modem.

Note The Cisco CMTS creates more than one RBG from a parent WB interface if the user has set aside more than one WB interface as the RBG and the RF bandwidth does not exceed 100%.

If a matching RBG is not found or cannot be created, the Cisco CMTS looks for an RBG with a subset of the required RF channels and if available, the cable modem is assigned to such an RBG.

However, if no such RBG exists, the Cisco CMTS instructs the line card to move the cable modem to NB mode.

For more information about NB mode, see Wideband Modem Resiliency.

How to Configure Downstream Resiliency Bonding Group

This section contains the following:

Enabling Downstream Resiliency Bonding Group

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rf-change-trigger** {**percent** *value* | **count** *number*} [**secondary**] **Example:** `Router(config)# cable rf-change-trigger percent 50 count 1 secondary`	Specifies the amount of time an event must persist before it triggers an action for the reporting CM. • **percent** *value*—Indicates the percentage of cable modems that must report a particular non-primary RF channel is down before that channel is removed from the bonding group. The valid range is 1 to 100. The default value is 0. • **count** *number*—Specifies the number of cable modems reporting an impairment for a non-primary downstream channel. The default value is 0. • **secondary**—(Optional) Configures the Cisco CMTS to move the unicast secondary service flows to the primary channel interface, when the

	Command or Action	Purpose
		number of cable modems reporting RF channel impairment is less than the configured (percent or count) threshold. **Note** Only those unicast secondary service flows, which share the same wideband interface as the primary interface, are moved to the primary channel interface. By default, the **secondary** keyword is not configured.
Step 4	**cable resiliency ds-bonding** **Example:** `Router(config)# cable resiliency ds-bonding`	Enables the downstream resiliency bonding group.
Step 5	**exit** **Example:** `Router(config)# exit`	Returns to the global configuration mode.

What to Do Next

Note The result of using the **cable rf-change-trigger** command with the **cable resiliency ds-bonding** command is different from using only the **cable rf-change-trigger** command. For more information, see Table 30: Wideband Modem Resiliency Versus Downstream Resiliency - Scenario 1 , on page 348 and Table 31: Wideband Modem Resiliency Versus Downstream Resiliency - Scenario 2 , on page 350. For more information, see Wideband Modem Resiliency .

Reserving a Resiliency Bonding Group for a Line Card

This section describes reserving a bonding group or a wideband interface for a line card per controller.

Restriction When you reserve a resiliency bonding group using the cable ds-resiliency command, the existing bundle and RF channel configurations on the wideband interface will be removed automatically. Other configurations like admission control, should be removed manually.

After downstream resiliency bonding group is configured, avoid other manual configurations.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** *slot*/{*subslot* | *bay*}/*port:wideband-channel* **Example:** `Router(config)# interface wideband-cable 1/0/0:7`	Configures a wideband cable interface. • *slot*—Slot where the cable line card resides. • *subslot*—Subslot where the cable line card resides. • *port*—Port number on the WB interface. • *wideband-channel*—WB interface on the router.
Step 4	**cable ds-resiliency** **Example:** `Router(config-if)# cable ds-resiliency`	Reserves an individual bonding group or WB interface for usage on a line card, on a per controller basis.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to the global configuration mode.

Verifying Downstream Resiliency Bonding Group Configuration

This section contains the following:

Verifying the Downstream Resiliency Bonding Group

To verify if the Downstream Resiliency Bonding Group feature is enabled, use the **show cable modem resiliency** command as shown in the following example:

```
Router# show cable modem resiliency
                                  Orig BG                Curr BG
I/F     MAC Address    ID   I/F           RFs ID   I/F           RFs
------- -------------- ---------------------- ----------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     4   898  Wi7/0/0:1     3
C7/0/0  0025.2eaf.8356 897  Wi7/0/0:0     4   899  Wi7/0/0:2     3
C7/0/0  0015.d176.5199 897  Wi7/0/0:0     4   720  In7/0/0:0
```

The **Current BG I/F** field indicates whether Downstream Resiliency Bonding Group feature is enabled and if the cable modems are assigned to a WB interface.

Verifying a Reserved Resiliency Bonding Group

To verify if a BG is reserved for a line card, use the **show cable resiliency** command as shown in the following example:

```
Router# show cable resiliency
                BG   Resil BG                                  RF
Resil BG I/F    ID   State          Count Time              Ctrl  Num
--------------- ---- -------------- ----- --------------- ----------
Wi1/2/0:10      10   Free
Wi1/2/0:20      20   Free
Wi7/0/0:1       1    Assigned       3     Nov 3  09:55:49 0     0
                                                                1
                                                                2
Wi7/0/0:2       2    Assigned       3     Nov 3  09:57:09 0     0
                                                                1
                                                                3
```

Wideband Modem Resiliency Versus Downstream Resiliency

This section provides the sample outputs when using the **cable rf-change-trigger** command with the **cable resiliency ds-bonding** command and using only the **cable rf-change-trigger** command.

Table 30: Wideband Modem Resiliency Versus Downstream Resiliency - Scenario 1

Effect on	Using only cable rf-change-trigger command (Wideband Modem Resiliency)		Using cable rf-change-trigger command with cable resiliency ds-bonding (Downstream Resiliency Bonding Group)	
	Below Threshold	**Above Threshold**	**Below Threshold**	**Above Threshold**
Primary Service Flow	Moves to the primary channel.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.	Moves to dynamic bonding group.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.
Secondary Service Flows	Remain on the original WB interface.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.	Remains on the original bonding group.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.

The following is a sample output for a cable modem when the **cable rf-change-trigger** command is used with the **cable resiliency ds-bonding** command and the number of cable modems observing an RF channel impairment is *below* the resiliency threshold:

```
Router# show cable modem

                                                                      D
MAC Address    IP Address     I/F           MAC           Prim RxPwr  Timing Num I
                                            State         Sid  (dBmv) Offset CPE P
0023.be83.1c9e 10.1.11.46     C5/0/0/UB     w-online      922  -0.50  1055   0   N
0023.be83.1caa 10.1.11.28     C5/0/0/UB     w-online      923  0.00   1043   0   N
```

```
0025.2ecf.f19c 10.1.11.53     C5/0/0/UB     w-online       925  0.00   1057   0   N
0022.3a30.9fc0 10.1.11.47     C5/0/0/UB     w-online       926  0.00   1055   0   N
001a.c3ff.e3d4 10.1.11.39     C5/0/0/UB     p-online       927  0.00   1307   0   N
0023.be83.1c9a 10.1.11.61     C5/0/0/UB     w-online       928  0.00   1057   0   N
0022.3a30.9fbc 10.1.11.60     C5/0/0/UB     p-online       929  -0.50  1055   0   N
0023.be83.1c8c 10.1.11.38     C5/0/0/UB     w-online       930  0.00   1061   0   N
001e.6bfb.1964 10.1.11.63     C5/0/0/UB     p-online       931  0.50   1305   0   N
0025.2ecf.f196 10.1.11.29     C5/0/0/UB     w-online       932  0.00   1057   0   N
0025.2ecf.f04e 10.1.11.54     C5/0/0/UB     w-online       933  0.00   1054   0   N
0022.3a30.9fc8 10.1.11.43     C5/0/0/UB     w-online       934  0.00   1056   0   N
0025.2ecf.f190 10.1.11.55     C5/0/0/UB     w-online       935  0.00   1059   0   N
0022.3a30.9fd0 10.1.11.52     C5/0/0/UB     p-online       936  0.00   1057   0   N
0022.ce97.8268 10.1.11.31     C5/0/0/UB     w-online       937  -0.50  1056   0   N
0022.ce97.8281 10.1.11.25     C5/0/0/UB     w-online       938  0.00   1058   0   N
001a.c3ff.e4ce 10.1.11.44     C5/0/0/UB     w-online       940  -0.50  1304   0   N
0022.ce9c.839e 10.1.11.32     C5/0/0/UB     w-online       941  -0.50  1305   0   N
0022.cea3.e768 10.1.11.41     C5/0/0/UB     w-online       942  -1.00  1305   0   N
0022.ce9c.8398 10.1.11.33     C5/0/0/UB     w-online       943  0.00   1306   0   N
001a.c3ff.e50a 10.1.11.59     C5/0/0/UB     w-online       944  0.00   1304   0   N
001a.c3ff.e3f8 10.1.11.57     C5/0/0/UB     w-online       945  -1.00  1306   0   N
001e.6bfb.1a14 10.1.11.37     C5/0/0/UB     w-online       946  0.00   1305   0   N
```

Note p-online indicates that the cable modem is in downstream partial service mode.

```
Router# show cable resiliency
                BG   Resil BG                                  RF
Resil BG I/F    ID   State           Count Time                Ctrl  Num
--------------- ---- --------------- ----- ------------------- ----  ---
Wi5/0/0:2       2    Assigned        1     Mar 30 14:46:43 0     0
                                                                   1
                                                                   2
Wi5/0/0:3       3    Assigned        1     Mar 30 14:46:43 0     0
                                                                   1
                                                                   2
                                                             1     0
                                                                   1
                                                                   2
                                                                   3
Wi5/0/0:4       4    Free            0
Wi5/0/0:5       5    Free            0

Router# show cable modem resiliency
                                Orig BG                 Curr BG
I/F     MAC Address    ID   I/F             RFs ID   I/F             RFs
------- -------------- ---- --------------- ---- ---- --------------- ----
C5/0/0  001a.c3ff.e3d4 258  Wi5/0/0:1       4    259  Wi5/0/0:2       3 <- Dynamic Bonding Group
C5/0/0  0022.3a30.9fbc 257  Wi5/0/0:0       8    260  Wi5/0/0:3       7 <- Dynamic Bonding Group
C5/0/0  001e.6bfb.1964 258  Wi5/0/0:1       4    259  Wi5/0/0:2       3 <- Dynamic Bonding Group
C5/0/0  0022.3a30.9fd0 257  Wi5/0/0:0       8    260  Wi5/0/0:3       7 <- Dynamic Bonding Group
```

The following is a sample output for a cable modem under the following conditions:

- **cable rf-change-trigger** command is used with the **cable resiliency ds-bonding** command
- Number of cable modems observing an RF channel impairment is *below* the resiliency threshold
- There is no available WB interface for the resiliency bonding group:

```
Router# show cable modem
 0025.2ecf.f196 service-flow version
SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num Primary    DS
                               Interface     State         Sid   CPE Downstream RfId
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     p-online
```

```
      932   0   In5/0/0:0  240
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
1867  US  act   932   BE     0    0           10000       0           294
1868  DS  act   N/A   N/A    0    0           3044        0           154

Router# show cable resiliency
                BG   Resil BG                                  RF
Resil BG I/F    ID   State          Count Time              Ctrl  Num
--------------- ---- -------------- ----- ----------------- ----------
Wi5/0/0:2       2    Assigned       6     Mar 30 15:57:09 0     0
                                                                 1
                                                                 2
                                                                 3
                                                           1     0
                                                                 2
                                                                 3
Wi5/0/0:3       3    Assigned       8     Mar 30 15:53:58 0     0
                                                                 1
                                                                 2
                                                           1     1
                                                                 2
                                                                 3
Wi5/0/0:4       4    Assigned       2     Mar 30 15:53:58 0     0
                                                                 1
                                                                 2
                                                                 3
                                                           1     1
                                                                 2
                                                                 3
Wi5/0/0:5       5    Assigned       2     Mar 30 15:58:35 0     0
                                                                 1
                                                                 2
                                                                 3
                                                           1     0
                                                                 1
                                                                 3

Router# show cable modem resiliency
                                  Orig BG                  Curr BG
I/F     MAC Address    ID   I/F           RFs ID   I/F           RFs
------- -------------- ---------------------- ---------------------
C5/0/0  0025.2ecf.f19c 257  Wi5/0/0:0     8   259  Wi5/0/0:2     7
C5/0/0  0025.2ecf.f196 257  Wi5/0/0:0     8   240  In5/0/0:0     <-- move NB for no available
 WB interface
C5/0/0  0025.2ecf.f04e 257  Wi5/0/0:0     8   262  Wi5/0/0:5     7
C5/0/0  0022.3a30.9fbc 257  Wi5/0/0:0     8   260  Wi5/0/0:3     6
C5/0/0  0022.3a30.9fd0 257  Wi5/0/0:0     8   261  Wi5/0/0:4     7
```

Table 31: Wideband Modem Resiliency Versus Downstream Resiliency - Scenario 2

Effect on	Using only cable rf-change-trigger secondary command (Wideband Modem Resiliency)		Using cable rf-change-trigger secondary command with cable resiliency ds-bonding (Downstream Resiliency Bonding Group)	
	Below Threshold	**Above Threshold**	**Below Threshold**	**Above Threshold**
Primary Service Flow	Moves all service flows to the primary channel.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.	Moves all service flows to a dynamic bonding group.	Remains on the original bonding group while the impaired downstream channels are not used and are reported as DOWN.
Secondary Service Flows				

The following is a sample output for a cable modem when the **cable rf-change-trigger secondary** command is used with the **cable resiliency ds-bonding** command and the number of cable modems observing an RF channel impairment is *below* the resiliency threshold:

```
Router# show cable modem 0025.2ecf.f196 service-flow
SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num Primary    DS
                               Interface     State         Sid   CPE Downstream RfId
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     p-online      955   0   In5/0/0:0  240
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
           State       Type
1913  US  act   955   BE     0    10000000    10000       0           425
1915  US  act   956   RTPS   7    0           3044        100000      0
1916  US  act   957   BE     0    0           3044        50000       0
1917  US  act   958   BE     4    0           3044        0           0
1914  DS  act   N/A   N/A    0    100000000   20000       0           0       <-- Primary
Service-Flow
1918  DS  act   N/A   N/A    0    0           3044        0           0       <-- Secondary
 Service-Flow
1919  DS  act   N/A   N/A    0    0           3044        0           0       <-- Secondary
 Service-Flow
1920  DS  act   N/A   N/A    4    4500000     3044        0           0       <-- Secondary
 Service-Flow
UPSTREAM SERVICE FLOW DETAIL:
SFID  SID   Requests   Polls      Grants     Delayed    Dropped    Packets
                                             Grants     Grants
1913  955   83         0          83         0          0          92
1915  956   0          0          0          0          0          0
1916  957   0          0          0          0          0          0
1917  958   0          0          0          0          0          0
DOWNSTREAM SERVICE FLOW DETAIL:
SFID  RP_SFID QID    Flg Policer              Scheduler              FrwdIF
                         Xmits      Drops      Xmits      Drops
1914  33210   131555     90         0          6          0          Wi5/0/0:3 <-- Dynamic
 Bonding Group
1918  33211   131556     0          0          0          0          Wi5/0/0:3
1919  33212   131557     0          0          0          0          Wi5/0/0:3
1920  33213   131558     0          0          0          0          Wi5/0/0:3
```

Troubleshooting the Downstream Resiliency Bonding Group Configuration

Use the following commands to get information on the WB interface, number of CMs in an impaired state, resiliency bonding groups, their associated bonding groups, available RF channels, and the number of CMS and service flows assigned to them:

- **debug cable wbcmts resiliency**
- **debug cable wbcmts resiliency report**
- **show cable resiliency**
- **show cable modem resiliency**
- **show cable modem wideband rcs-status**
- **show cable modem service-flow verbose**
- **show cable rf-status**
- **show cable modem summary wb-rfs**

Configuration Examples of the Downstream Resiliency Bonding Group Feature

The following is an example of the configuration of the Downstream Resiliency Bonding Group feature on a Cisco UBR-MC20X20V line card:

```
controller Integrated-Cable 5/0/0
rf-channel 0 frequency 387000000 annex B modulation 256qam interleave 32
 rf-channel 0 rf-power 52.0
 no rf-channel 0 rf-shutdown
rf-channel 1 frequency 393000000 annex B modulation 256qam interleave 32
 rf-channel 1 rf-power 52.0
 no rf-channel 1 rf-shutdown
rf-channel 2 frequency 399000000 annex B modulation 256qam interleave 32
 rf-channel 2 rf-power 52.0
 no rf-channel 2 rf-shutdown
rf-channel 3 frequency 405000000 annex B modulation 256qam interleave 32
 rf-channel 3 rf-power 52.0
 no rf-channel 3 rf-shutdown
interface Cable5/0/0
 downstream Integrated-Cable 5/0/0 rf-channel 0
 cable mtc-mode
 cable bundle 1
  cable upstream bonding-group 510
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes 80000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 17000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 1
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 frequency 24000000
 cable upstream 1 channel-width 6400000 6400000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 1
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 frequency 31000000
 cable upstream 2 channel-width 6400000 6400000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 1
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 frequency 38000000
 cable upstream 3 channel-width 6400000 6400000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 1
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 no cable upstream 3 shutdown
interface Integrated-Cable5/0/0:0
 cable bundle 1
 cable rf-bandwidth-percent 10
!
interface Wideband-Cable5/0/0:0
cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
```

```
 cable rf-channel 3 bandwidth-percent 10
 cable rf-channel controller 1 channel 0 bandwidth-percent 10
 cable rf-channel controller 1 channel 1 bandwidth-percent 10
 cable rf-channel controller 1 channel 2 bandwidth-percent 10
 cable rf-channel controller 1 channel 3 bandwidth-percent 10
!
interface Wideband-Cable5/0/0:1
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
!
interface Wideband-Cable5/0/0:2
 cable ds-resiliency
!
interface Wideband-Cable5/0/0:3
 cable ds-resiliency
!
interface Wideband-Cable5/0/0:4
 cable ds-resiliency
!
interface Wideband-Cable5/0/0:5
 cable ds-resiliency

cable fiber-node 50
 downstream Integrated-Cable 5/0/0 rf-channel 0-3
 downstream Integrated-Cable 5/0/1 rf-channel 0-3
 upstream Cable 5/0 connector 0-3
```

The following is an example of the configuration of the Downstream Resiliency Bonding Group feature with multiple Cisco UBR-MC20X20V line cards:

- Primary bonding group on the Cisco UBR-MC20X20V line card in slot 7/1
- Another bonding group on the Cisco UBR-MC20X20V line card in slot 8/1
- Resiliency Bonding Group is set aside on the Cisco UBR-MC20X20V line card in slot 7/1

```
interface Wideband-Cable7/1/0:0
 cable bundle 2
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
!
interface Wideband-Cable8/1/3:0
 cable bundle 2
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
!
interface Wideband-Cable7/1/0:3
cable ds-resiliency
!
interface Wideband-Cable7/1/0:4
cable ds-resiliency
interface Wideband-Cable8/1/3:3
cable ds-resiliency
!
interface Wideband-Cable8/1/3:4
cable ds-resiliency
```

The following is an example of the cross-controller configuration of the Downstream Resiliency Bonding Group feature with the Cisco UBR-MC20X20 line card:

```
interface Wideband-Cable8/1/3:2
```

```
 cable bundle 3
 cable rf-channel controller 1 channel 0 bandwidth-percent 10
 cable rf-channel controller 1 channel 1 bandwidth-percent 10
 cable rf-channel controller 1 channel 2 bandwidth-percent 10
 cable rf-channel controller 1 channel 3 bandwidth-percent 10
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
!
!
interface Wideband-Cable8/1/3:3
 cable ds-resiliency
!
interface Wideband-Cable8/1/3:4
 cable ds-resiliency
!
```

The following is an example of the configuration of the Downstream Resiliency Bonding Group feature with a shared port adapter (SPA):

```
interface Wideband-Cable1/2/0:0
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 25
 cable rf-channel 1 bandwidth-percent 25
 cable rf-channel 2 bandwidth-percent 25
 cable rf-channel 3 bandwidth-percent 25
!
interface Wideband-Cable1/2/0:3
 cable ds-resiliency
!
interface Wideband-Cable1/2/0:4
 cable ds-resiliency
|
```

The following is a sample output for the **show cable modem** command to display impaired CMs below the resiliency threshold value:

```
Router# show cable modem
                                                                          D
MAC Address    IP Address     I/F           MAC           Prim RxPwr  Timing Num I
                                            State         Sid  (dBmv) Offset CPE P
0023.be83.1c9e 10.1.11.46     C5/0/0/UB     w-online      922  -0.50  1055   0   N
0023.be83.1caa 10.1.11.28     C5/0/0/UB     w-online      923  0.00   1043   0   N
0025.2ecf.f19c 10.1.11.53     C5/0/0/UB     w-online      925  0.00   1057   0   N
0022.3a30.9fc0 10.1.11.47     C5/0/0/UB     w-online      926  0.00   1055   0   N
001a.c3ff.e3d4 10.1.11.39     C5/0/0/UB     p-online      927  0.00   1307   0   N
0023.be83.1c9a 10.1.11.61     C5/0/0/UB     w-online      928  0.00   1057   0   N
0022.3a30.9fbc 10.1.11.60     C5/0/0/UB     p-online      929  -0.50  1055   0   N
0023.be83.1c8c 10.1.11.38     C5/0/0/UB     w-online      930  0.00   1061   0   N
001e.6bfb.1964 10.1.11.63     C5/0/0/UB     p-online      931  0.50   1305   0   N
0025.2ecf.f196 10.1.11.29     C5/0/0/UB     w-online      932  0.00   1057   0   N
0025.2ecf.f04e 10.1.11.54     C5/0/0/UB     w-online      933  0.00   1054   0   N
0022.3a30.9fc8 10.1.11.43     C5/0/0/UB     w-online      934  0.00   1056   0   N
0025.2ecf.f190 10.1.11.55     C5/0/0/UB     w-online      935  0.00   1059   0   N
0022.3a30.9fd0 10.1.11.52     C5/0/0/UB     p-online      936  0.00   1057   0   N
0022.ce97.8268 10.1.11.31     C5/0/0/UB     w-online      937  -0.50  1056   0   N
0022.ce97.8281 10.1.11.25     C5/0/0/UB     w-online      938  0.00   1058   0   N
001a.c3ff.e4ce 10.1.11.44     C5/0/0/UB     w-online      940  -0.50  1304   0   N
0022.ce9c.839e 10.1.11.32     C5/0/0/UB     w-online      941  -0.50  1305   0   N
0022.cea3.e768 10.1.11.41     C5/0/0/UB     w-online      942  -1.00  1305   0   N
0022.ce9c.8398 10.1.11.33     C5/0/0/UB     w-online      943  0.00   1306   0   N
001a.c3ff.e50a 10.1.11.59     C5/0/0/UB     w-online      944  0.00   1304   0   N
001a.c3ff.e3f8 10.1.11.57     C5/0/0/UB     w-online      945  -1.00  1306   0   N
001e.6bfb.1a14 10.1.11.37     C5/0/0/UB     w-online      946  0.00   1305   0   N
```

Note p-online indicates that the CM is in downstream partial service mode.

When the impaired CMs have recovered, the **show cable modem** command displays the following output:

```
Router# show cable modem
MAC Address    IP Address      I/F           MAC           Prim RxPwr  Timing Num I
                                             State         Sid  (dBmv) Offset CPE P
0023.be83.1c9e 10.1.11.46      C5/0/0/UB     w-online      922  -0.50  1055   0   N
0023.be83.1caa 10.1.11.28      C5/0/0/UB     w-online      923  0.00   1043   0   N
0025.2ecf.f19c 10.1.11.53      C5/0/0/UB     w-online      925  0.50   1057   0   N
0022.3a30.9fc0 10.1.11.47      C5/0/0/UB     w-online      926  -0.50  1055   0   N
001a.c3ff.e3d4 10.1.11.39      C5/0/0/UB     w-online      927  0.00   1307   0   N
0023.be83.1c9a 10.1.11.61      C5/0/0/UB     w-online      928  0.00   1057   0   N
0022.3a30.9fbc 10.1.11.60      C5/0/0/UB     w-online      929  -0.50  1055   0   N
0023.be83.1c8c 10.1.11.38      C5/0/0/UB     w-online      930  0.00   1061   0   N
001e.6bfb.1964 10.1.11.63      C5/0/0/UB     w-online      931  0.50   1305   0   N
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     w-online      932  0.00   1057   0   N
0025.2ecf.f04e 10.1.11.54      C5/0/0/UB     w-online      933  0.00   1054   0   N
0022.3a30.9fc8 10.1.11.43      C5/0/0/UB     w-online      934  0.00   1056   0   N
0025.2ecf.f190 10.1.11.55      C5/0/0/UB     w-online      935  0.00   1059   0   N
0022.3a30.9fd0 10.1.11.52      C5/0/0/UB     w-online      936  0.00   1057   0   N
0022.ce97.8268 10.1.11.31      C5/0/0/UB     w-online      937  -1.00  1056   0   N
0022.ce97.8281 10.1.11.25      C5/0/0/UB     w-online      938  0.00   1058   0   N
001a.c3ff.e4ce 10.1.11.44      C5/0/0/UB     w-online      940  -0.50  1304   0   N
0022.ce9c.839e 10.1.11.32      C5/0/0/UB     w-online      941  -0.50  1305   0   N
0022.cea3.e768 10.1.11.41      C5/0/0/UB     w-online      942  -1.00  1305   0   N
0022.ce9c.8398 10.1.11.33      C5/0/0/UB     w-online      943  -0.50  1306   0   N
001a.c3ff.e50a 10.1.11.59      C5/0/0/UB     w-online      944  -0.50  1304   0   N
001a.c3ff.e3f8 10.1.11.57      C5/0/0/UB     w-online      945  0.50   1306   0   N
001e.6bfb.1a14 10.1.11.37      C5/0/0/UB     w-online      946  0.00   1305   0   N
```

The following is a sample output for the **show cable modem** command to display impaired CMs above the resiliency threshold value:

```
Router# show cable modem
                                                                                 D
MAC Address    IP Address      I/F           MAC           Prim RxPwr  Timing Num I
                                             State         Sid  (dBmv) Offset CPE P
4458.294a.f3cc 10.1.11.27      C5/0/0/U3     init(o)       1020 0.00   1053   0   N
001e.6bfb.1964 10.1.11.63      C5/0/0/UB     w-online      1021 0.00   1305   0   N
0022.3a30.9fc0 10.1.11.47      C5/0/0/UB     p-online      1022 -0.50  1056   0   N
001a.c3ff.e3f8 10.1.11.57      C5/0/0/UB     p-online      1023 0.00   1305   0   N
0025.2ecf.f190 10.1.11.55      C5/0/0/UB     p-online      1027 0.00   1056   0   N
001a.c3ff.e4ce 10.1.11.44      C5/0/0/UB     p-online      1031 -0.50  1306   0   N
0022.ce9c.8398 10.1.11.33      C5/0/0/UB     p-online      1032 -0.50  1305   0   N
0025.2ecf.f04e 10.1.11.54      C5/0/0/UB     p-online      1039 -1.00  1056   0   N
0022.3a30.9fbc 10.1.11.60      C5/0/0/UB     w-online      1040 0.00   1055   0   N
001a.c3ff.e3d4 10.1.11.39      C5/0/0/UB     w-online      1041 0.00   1305   0   N
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     p-online      1042 -1.00  1058   0   N
0025.2ecf.f19c 10.1.11.53      C5/0/0/UB     p-online      1043 0.00   1058   0   N
0022.3a30.9fd0 10.1.11.52      C5/0/0/UB     w-online      1047 -0.50  1059   0   N
0023.be83.1c8c 10.1.11.38      C5/0/0/UB     p-online      1051 0.00   1057   0   N
0022.3a30.9fc8 10.1.11.43      C5/0/0/UB     p-online      1061 -0.50  1056   0   N
0023.be83.1c9e 10.1.11.46      C5/0/0/UB     p-online      1065 0.00   1060   0   N
0023.be83.1caa 10.1.11.28      C5/0/0/UB     p-online      1069 0.00   1049   0   N
001a.c3ff.e50a 10.1.11.59      C5/0/0/UB     p-online      1070 -0.50  1306   0   N
0023.be83.1c9a 10.1.11.61      C5/0/0/UB     p-online      1071 0.00   1056   0   N
0022.ce9c.839e 10.1.11.32      C5/0/0/UB     p-online      1078 -1.00  1305   0   N
0022.cea3.e768 10.1.11.41      C5/0/0/UB     p-online      1079 0.00   1306   0   N
001e.6bfb.1a14 10.1.11.37      C5/0/0/UB     p-online      1089 0.00   1304   0   N
0022.ce97.8268 10.1.11.31      C5/0/0/UB     p-online      1102 -0.50  1058   0   N
0022.ce97.8281 10.1.11.25      C5/0/0/UB     p-online      1103 0.00   1056   0   N
```

The following is a sample of output for the **show cable resiliency** command that displays that resiliency bonding groups are free:

```
Router# show cable resiliency
              BG   Resil BG                                  RF
Resil BG I/F  ID   State          Count Time            Ctrl  Num
------------- ---- -------------- ----- --------------- ----------
Wi5/0/0:2     2    Free           9     Mar 30 17:18:21
Wi5/0/0:3     3    Free           9     Mar 30 16:22:21
Wi5/0/0:4     4    Free           2     Mar 30 15:53:58
Wi5/0/0:5     5    Free           3     Mar 30 16:24:12
```

The Cisco CMTS creates more than one RBG from a parent WB interface if the user has set aside more than one WB interface as an RBG and the RF bandwidth does not exceed 100 percent.

In the following example:

- Parent WB interface—wideband-cable 1/2/0:0
- RBGs—wideband-cable1/2/0:3, wideband-cable1/2/0:4, and wideband-cable1/2/0:5

```
!
interface Wideband-Cable1/2/0:0
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 25
 cable rf-channel 1 bandwidth-percent 25
 cable rf-channel 2 bandwidth-percent 25
 cable rf-channel 3 bandwidth-percent 25
end
!
interface Wideband-Cable1/2/0:3
 cable ds-resiliency
end
!
interface Wideband-Cable1/2/0:4
 cable ds-resiliency
end
!
interface Wideband-Cable1/2/0:5
 cable ds-resiliency
end
```

```
Router# show cable resiliency

              BG   Resil BG                                  RF
Resil BG I/F  ID   State          Count Time            Ctrl  Num
------------- ---- -------------- ----- --------------- ----------
Wi1/2/0:3     3    Free           1     May 24 09:58:35
Wi1/2/0:4     4    Free           0
Wi1/2/0:5     5    Free           0
Router# show cable modem resiliency

                              Orig BG                Curr BG
I/F     MAC Address    ID   I/F           RFs ID   I/F           RFs
------- -------------- ---- ---------------------- ----------------------
Router# show cable modem c7/0/0
                                                                          D
MAC Address    IP Address     I/F           MAC           Prim RxPwr  Timing Num I
                              State         Sid  (dBmv) Offset CPE  P
001e.6bfc.d732 80.66.0.16     C7/0/0/U0     w-online      1    0.00   1989   0   N
0025.2e2d.74cc 80.66.0.14     C7/0/0/U1     w-online      5    0.00   1592   1   N
0025.2ebf.29dd 80.66.0.3      C7/0/0/U0     w-online      10   0.50   1591   0   N
0015.d176.5b9d 80.66.0.15     C7/0/0/U0     w-online      17   0.75   1990   0   N
```

In the following example, CM1 reports RF 1 failure, CM2 reports RF 2 failure, and CM3 reports RF 3 failure. In this case, three RBGs are created:

```
Router# show cable resiliency
              BG   Resil BG                                    RF
Resil BG I/F  ID   State          Count Time              Ctrl  Num
------------- ---- -------------- ----- ----------------- ----------
Wi1/2/0:3     3    Assigned       2     May 24 10:39:42 2     0
                                                               2
                                                               3
Wi1/2/0:4     4    Assigned       1     May 24 10:39:42 2     0
                                                               1
                                                               3
Wi1/2/0:5     5    Assigned       1     May 24 10:39:42 2     0
                                                               1
                                                               2

Router# show cable modem resiliency
                                Orig BG                 Curr BG
I/F     MAC Address     ID   I/F            RFs ID   I/F            RFs
------- -------------- ---- ---------------------- ----------------------
C7/0/0  001e.6bfc.d732 65   Wi1/2/0:0      4   68   Wi1/2/0:3      3
C7/0/0  0025.2e2d.74cc 65   Wi1/2/0:0      4   69   Wi1/2/0:4      3
C7/0/0  0025.2ebf.29dd 65   Wi1/2/0:0      4   70   Wi1/2/0:5      3
!
interface Wideband-Cable1/2/0:3
 cable bundle 1
 cable ds-resiliency
 cable rf-channel 0 bandwidth-percent 1
 cable rf-channel 2 bandwidth-percent 1
 cable rf-channel 3 bandwidth-percent 1
end
!
interface Wideband-Cable1/2/0:4
 cable bundle 1
 cable ds-resiliency
 cable rf-channel 0 bandwidth-percent 1
 cable rf-channel 1 bandwidth-percent 1
 cable rf-channel 3 bandwidth-percent 1
end
!
interface Wideband-Cable1/2/0:5
 cable bundle 1
 cable ds-resiliency
 cable rf-channel 0 bandwidth-percent 1
 cable rf-channel 1 bandwidth-percent 1
 cable rf-channel 2 bandwidth-percent 1
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS Command Reference	http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Wideband Modem Resiliency	http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ ubr_wm_resiliency.html

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

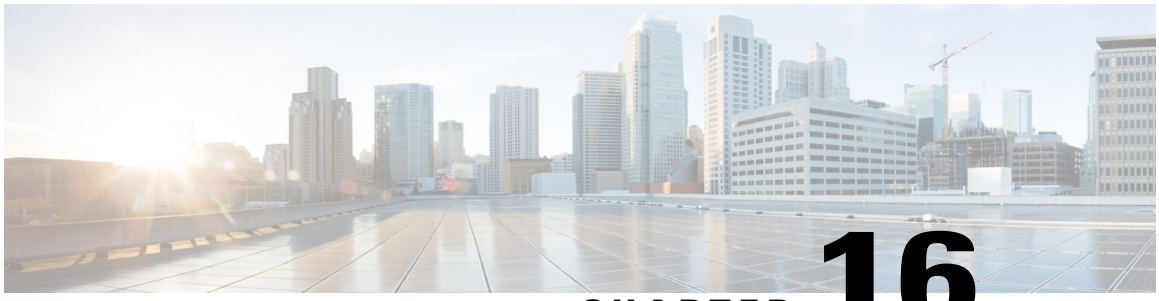
Feature Information for Downstream Resiliency Bonding Group

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 32: Feature Information for Downstream Resiliency Bonding Group

Feature Name	Releases	Feature Information
Downstream Resiliency Bonding Group	12.2(33)SCG	This feature was introduced. The following commands were introduced: • **cable resiliency ds-bonding** • **cable ds-resiliency** • **show cable modem resiliency** • **show cable resiliency**



CHAPTER 16

IGMP-Triggered Dynamic Channel Change Load Balancing for DOCSIS 2.0 Cable Modems

First Published: June 20, 2011

Last Updated: September 8, 2011

The Internet Group Management Protocol (IGMP) Triggered Dynamic Channel Change (DCC) Load Balancing (LB) feature is introduced to avoid rejection of new video streams either due to bandwidth constraints or repeated admission control failures on an interface.

If there are admission control failures during a session request, the load balancing infrastructure provides a list of downstream channels to which the cable modem (CM) can be moved. Downstream channels that already carry the existing session replication are given preference.

Note This feature is supported only on DOCSIS 2.0 CMs and DOCSIS 3.0 CMs operating in narrowband (NB) mode.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

The IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2(33)SCF and later releases. The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 33: IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs – Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2[21] • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20U/H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[22]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC88V [23]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC88V

21 PRE = Performance Routing Engine

22 The Cisco uBR-MC3GX60V cable interface line card is compatible only with PRE4.

23 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Software Prerequisites

- The IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs feature is enabled on every CM based on the load balancing policy.

- Load balancing infrastructure ensures that the CM is assigned to the intended load balancing group (LBG).
- CM is moved during session setup depending on the existing multicast replications and bandwidth requirements.
- CM cannot move the downstream channels that are forwarding any voice or video traffic if any active sessions are being forwarded on that CM.
- Route processor and line card high availability is supported.

Restrictions for IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

- IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs feature is only supported on NB CMs.
- When an IGMP-triggered DCC load balancing request is sent to the Cisco CMTS, the route processor (RP) queues the request and performs admission control checks and processes the request only if the result is a success.
- CMs with an active stream are not moved.
- DOCSIS 3.0 that are wideband (WB) CMs will not be moved for any optimization.
- Downstream selection and attribute checking is performed on the host line card for multicast sessions.
- For NB DOCSIS 2.0 and DOCSIS 3.0 modems that are either Multicast DSID Forwarding (MDF) enabled or MDF-disabled, combined optimization technique is applied at the time of session request. For more information, see Combined Optimization Technique, on page 361.
- Encrypted multicast streams are not supported in IGMP-triggered DCC load balancing.

Information About IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

IGMP-triggered DCC load balancing for DOCSIS 2.0 CM ensures that new video streams are not rejected due to multiple admission control failures. This solution leverages the DOCSIS 3.0 load balancing infrastructure to identify a subset of downstream channels where the CMs can be moved. The downstream channel that is already carrying the existing session replication is preferred over other channels and the CM is moved to this channel to avoid further replication.

If no other downstream channel carries this video stream or does not support the required bandwidth, the CM is moved to a new downstream channel based on the downstream channel in the DCC request for DOCSIS 2.0 CMs—for CMs to be moved across MAC domains.

The following sections describe the technique used to load balance CMs, and the interaction of the IGMP-Triggered DCC Load Balancing feature with DOCSIS LB and Fairness Across DOCSIS Interfaces:

Combined Optimization Technique

The IGMP-Triggered DCC Load Balancing feature combines replication-based and bandwidth-based optimization techniques to decide when and how load balancing take place.

Replication-based optimization—This technique minimizes the number of active replications by load balancing a CM to a downstream where the replications exits.

Bandwidth-based optimization—If a new replication needs to be created and the current downstream channel cannot handle the replication request due to insufficient committed information rate (CIR) bandwidth, the CM will be load balanced to a downstream that has the lowest CIR usage.

The combined optimization technique follows these rules:

- When a session request comes in, the replication-based optimization technique is given preference.
- When there are second streams and best effort (BE) traffic on the same bonding group (BG), the weighted RF utilization is measured before making a decision about whether a new replication should be created.
- If there are no existing replications or a new replication needs to be created, the bandwidth-based technique is used to move the CM to a new BG.
- For unicast sessions, the CIR bandwidth-based approach is used.

Note The IGMP-Triggered DCC Load Balancing feature is not supported for unicast sessions for Cisco IOS Release 12.2(33)SCF.

- When there are multiple overlapping BGs carrying the replication, no preference is given based on size.

Session Creation Request

When a new session request is received, the IGMP-Triggered DCC Load Balancing feature moves CMs when:

- IGMP-triggered DCC load balancing is configured.
- There are no PacketCable Multimedia (PCMM) based multicast flows.
- There are no non-zero CIR unicast or IGMP-based multicast flows on the downstream channel.

The following rules apply during admission control decisions for the session replication request:

- For multicast session requests, the downstream channels carrying the existing replications are the primary candidates if:
  - The forwarding interface is a subset of the current downstream channels or receive channel configuration (RCC) of the CM. In this case, the CM is automatically assigned to the existing multicast session.
  - The replication is forwarding on an interface that is a subset of the LBG of the CM. In this case, the CM is moved to the candidate downstream channel.
- If the utility-based threshold is reached, such that non-video traffic is significantly affected, a new replication is created irrespective of an existing replication.

Note Static multicast sessions are handled in the same way as dynamic sessions with an existing session replication.

The following rules apply when a new session replication is required to be created:

- A new session replication is created if its admission to the current downstream channel interfaces passes.

- If the new session replication admission fails, the downstream channels in the LBG of the CM are searched for target downstream channels. This search is to find the forwarding interface with the least-utilized CIR.

If no new candidates are found, the session replication creation fails and the request is rejected.

Deployment of the IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 and DOCSIS 3.0 CMs

In an HFC plant with DOCSIS 2.0 and DOCSIS 3.0 CMs, the following points should be noted:

- Downstream forwarding to all DOCSIS 2.0 and NB CMs is done using cable, modular-cable (MC), and integrated-cable (IC) interfaces.

Note Cable interfaces on the Cisco uBR10-MC5X20 cable interface line card that use MDF are not supported.

- While using MC and IC interfaces for downstream forwarding, it is crucial to ensure that the configured **rf-bandwidth-percentage** is sufficient to serve the need for that interface.
- DOCSIS 3.0 CMs in wideband mode can receive traffic that is forwarded on all interfaces whose downstream channels are a subset of the RCC of the CM. However, by default forwarding always occur on the corresponding wideband interface. To forward downstream data on the MC and IC interface, configure specific attributes-based forwarding.

The following rules apply to multicast forwarding selection with IGMP-Triggered DCC load balancing feature in the following hybrid environments:

- For DOCSIS 3.0 CMs:
  - The existing replication is used if the session replication exists on a downstream channel that is subset of the RCC of the CM and the flow attribute matches the existing replication flow.
  - A new replication is created when the session replication exists on a downstream channel that is subset of the RCC of the CM, but the flow attributes do not match the existing replication flow.
  - A new replication is created if the session replication does not exists on a downstream channel that is subset of the RCC of the CM, but exists on a downstream channel that is a subset of the LBG of the CM.
  - If the session replication does not exist, but the flow attributes specifically point to a particular downstream channel, then the first downstream to match the attribute requirements along with the admission criteria of the flow is used for the forwarding. If the attributes match the BG and downstream channel, then than the BG is used for forwarding.
- For DOCSIS 2.0 CMs:
  - Existing replication is used if the session replication already exists on a downstream channel that is a subset of the LBG of the CM. For more information, see Session Creation Request, on page 362.
  - New replication is created if the session replication already exists on a BG that is a subset of the LBG of the CM.

Interaction of IGMP-Triggered DCC Load Balancing With DOCSIS Load Balancing

DOCSIS load balancing is based on the following methods that the Cisco CMTS uses to determine when interfaces are balanced:

- Modems method
- Service-flow method
- Utilization method

For more information on these DOCSIS LB methods, see Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers .

A single load balance group is used for both the DOCSIS and IGMP-triggered DCC load balancing. DOCSIS load balancing decisions are made during CM registration (static load balancing) as well as after registration (dynamic load balancing; depending on traffic conditions) to achieve a balanced system. IGMP-triggered DCC load balancing is triggered at the time of a video request.

CMs with active video-over-DOCSIS (VDOC) sessions are excluded from moving during the periodic dynamic balancing by DOCSIS load balancing. This can lead to situations where due to the number of CMs with active video session and the pattern of the usage, the interface is unbalanced. However, it is possible to have an unbalanced, but stable state based on the DOCSIS load balancing criteria.

- CMs with active video sessions are counted in the DOCSIS load balancing statistics, but are not allowed to move.
- IGMP-triggered DCC load balancing decisions are independent of the DOCSIS load balancing criteria.

show cable load-balance vdoc and **show cable load-balance docsis-group vdoc** commands provide detailed information on the state of the IGMP-triggered DCC load balancing for a particular LBG. These commands also include information to display why a non-balanced stable state is achieved.

Interaction of IGMP-Triggered DCC Load Balancing With Fairness Across DOCSIS Interfaces

CIR is the average available bandwidth under normal conditions. There may be an allowance of burstable bandwidth, known as the excess information rate (EIR). The connection always supports the CIR rate, and sometimes the EIR rate, provided there is adequate bandwidth. The CIR plus EIR is either equal to or less than the speed of the access port into the network.

The bandwidth allocation for BE traffic among BGs depends on:

- Statically configured bandwidth percentage
- Actual amount of admitted CIR
- Statically configured remaining ratio

Although the "remaining ratio" is meant for the bandwidth provisioning for the BE traffic, the actual amount of bandwidth used by the BE traffic depends on all three of the above factors.

So, the purpose is to adjust the guaranteed BG bandwidth adaptively to accommodate the CIR flow request by moving guaranteed bandwidth between the adjacent BGs (those that share RF channels). This is referred to as Adaptive CIR. After satisfying the CIR requests, the BG bandwidth is further adjusted based on the estimated traffic and active BE service flow count weighted by DOCSIS priority, so that flows with the same

traffic priority get the same amount of bandwidth across BGs. This is referred to as EIR Fairness. The solution as a whole is called Fairness Across DOCSIS Interfaces.

For the IGMP-triggered DCC load balancing to work seamlessly with Fairness Across DOCSIS Interfaces, it relies on the non-guaranteed bonus bandwidth for each BG to determine the threshold and BG capacity.

Note For NB and DOCSIS 3.0 load balancing operations, admission control does not utilize non-guaranteed bonus bandwidth for load balancing checks.

Therefore, if the admission control check passes, the probability that the service flow creation fails due to insufficient bandwidth is fairly low considering the requests will be serially processed.

Restrictions

- Because the host MAC domain does not have the complete information when the BG is shared across multiple MAC domains, due to bandwidth fragmentation in the service flow admission control (SFAC), admission control may fail even though the CIR bandwidth is available on the BG.
- Because the CIR bandwidth information is sent from the active route processor to the host MAC domain with the keepalives, the information is out of synchronization by 2 seconds. This may cause a race condition of possible incomplete or inaccurate knowledge at the time of the session creation.
- When Fairness Across DOCSIS Interfaces is configured, the MAC domain hosts must have the non-guaranteed bonus bandwidth information per bucket, per BG.
- For multicast sessions, there is a possibility that although a CM was moved to a different downstream to satisfy bandwidth requirements, the flow is rejected even though admission control had passed. The race condition here being that the bandwidth has been allocated to other flows in the meantime.

DOCSIS 2.0 Multicast Enhancement for VDOC

This feature enables you to tune a DOCSIS 2.0 CM to a specific downstream and supports static and dynamic multicast video forwarding on it. The vdoc-enabled keyword enables the VDOC load balancing for static multicast groups.

The set-top boxes (STB) are configured with static video streams. The Cisco CMTS will check if the CMs that are connected to these STBs are already on the specific downstream interface with these multicast replications when the Cisco CMTS receives joins for these static streams. If the CMs are not on the correct downstreams, then a DCC message is sent to the line card to initiate the CM to move to the correct downstream interface.

Static multicast sessions are not a MUST to enable this rule. The CM(s) can be moved to use an existing replication, static or dynamic with preference being given to static flows.

This feature has the following restrictions:

- This feature is not supported on LBGs, which are derived from fiber node configuration and with multicast encryption.
- This feature does not support logical upstream channels.
- This feature works with DOCSIS 2.0 and NB DOCSIS 3.0 CMs, which are MDF-enabled.
- For MDF-enabled CMs, the CM may support DCC but do not receive traffic till the next join arrives.

- Multicast quality of service (QoS) must be configured either globally or on the bundle interface.
- The CMs that support DCC due to load-balancing will use initialization technique 0 irrespective of the initialization technique configured on the LBG.
- This feature does not support multicast encryption. However, if the static group is configured for multicast encryption, then this feature will process the join and move the CM if required.

How to Configure IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

The following sections describe how to create and configure LBGs to enable load balancing on the Cisco CMTS. Each task is marked as required or optional, as appropriate.

Creating a Load Balancing Group

This section describes how to create an LBG. You must create at least one LBG before the Cisco CMTS can begin load balancing CMs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance group** *n* **method** [**modems** | **service-flows** | **utilization**] **Example:** `Router(config)# cable load-balance group 10 method service-flows`	Creates an LBG with the following parameters: • *n*—Number of the LBG. In Cisco IOS Release 12.2(33)SCE3 and earlier, the valid range is from 1 to 80. In Cisco IOS Release 12.2(33)SCE4 and later releases, the valid range is from 1 to 256. **Note** If downstream channels are not included in an LBG, then each downstream channel can be considered a separate domain. • **modems—**(Optional) Specifies that the LBG should use the number of active CMs on an interface to determine the current load (default). • **service-flows—**(Optional) Specifies that the LBG should use the number of active service flow IDs (SFIDs) on an interface to determine the current load. • **utilization—**(Optional) Specifies that the LBG should use the current percentage of utilization on an interface to determine the current load. (To avoid unnecessary movement of CMs, the utilization method does not

	Command or Action	Purpose
		perform load balancing until the amount of utilization on an interface is at 25 percent or more.)
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating a Load Balancing Rule

This configuration is optional. This section describes how to create a load balancing rule. You must create at least one load balancing rule before the Cisco CMTS can use load balancing policies.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-enable** **Example:** `Router(config)# cable load-balance docsis-enable`	Enables DOCSIS load balancing on the Cisco CMTS.
Step 4	**cable load-balance rule** *rule-id* **vdoc-enabled** **Example:** `Router(config)# cable load-balance rule 1 vdoc-enabled`	Creates a rule that prevents a CM from disabling or enabling load balancing. • **vdoc-enabled—**Enables the VDOC LB for static and dynamic multicast groups. • *rule-id*—Rule ID of the rule to load balance CM
Step 5	**cable load-balance docsis-policy** *policy-id* **rule** *rule-id* **Example:** `Router(config)# cable load-balance docsis-policy 1 rule 1`	Creates a DOCSIS policy and associates an existing rule with the policy. • *policy-id*—DOCSIS policy to be created. • **rule** *rule-id*—Specifies the rule to be used with the DOCSIS policy.

	Command or Action	Purpose
Step 6	**cable load-balance docsis-group** *docsis-group-id* **index** **Example:** `Router(config)# cable load-balance docsis-group 1 index 81`	Configures a DOCSIS LBG on the Cisco CMTS. • *docsis-group-id*—DOCSIS LBG ID. A valid DOCSIS LBG ID ranges from 1 to 2147483647 and does not overlap with the legacy LBG ID.
Step 7	**downstream Modular-Cable** *slot/subslot/controller* **rf-channel** *rf-channel* **Example:** `Router(config-lb-group)# downstream Modular-Cable 5/0/0 rf-channel 0-11`	Associates a set of upstreams with individual modular cable downstream channels into a given cable MAC domain. • *slot*—Cable interface slot. The valid values range from 5 to 8. • *subslot*—Cable interface subslot. The valid values are 0 or 1. • *controller*—Modular-cable controller number. The valid values range from 0 to 2. • **rf-channel**—Specifies the association of a continuous range of RF channels within the downstream. • *rf channels*—Range of RF channel physical ports.
Step 8	**downstream cable** *slot/subslot/controller* **Example:** `Router(config-lb-group)# downstream Cable 7/0/0`	Assigns a primary downstream channel for a fiber node. • *slot*—Cable interface slot. The valid values range from 5 to 8. • *subslot*—Cable interface subslot. The valid values are 0 or 1. • *controller*—Modular-cable controller number. The valid values range from 0 to 2.
Step 9	**upstream cable** *slot/subslot/port upstream-list* **Example:** `Router(config-lb-group)# upstream cable 7/0/0 0`	Sets upstream channels in a DOCSIS LBG. • **cable***slot/subslot/port*—Specifies the Cisco CMTS interface slot, subslot, and port number parameters. ◦ *slot*—Cable interface slot. The valid values range from 5 to 8. ◦ *subslot*—Cable interface subslot. The valid values are 0 and 1. ◦ *port*—Modular-Cable controller number. The valid values are 0 to 2. • *upstream-list*—Upstream channel list ranging from 0 to 7.
Step 10	**init-tech-list** *grouplist* [**ucc**] **Example:** `Router(config-lb-group)# init-tech-list 1`	Sets the DCC initialization techniques that the Cisco CMTS can use for load balancing CMs. • *grouplist*—DCC initialization technique list. **Note** It is not recommended to use init-tech-list 0.

	Command or Action	Purpose
		• **ucc—**(Optional) Determines whether Upstream Channel Change (UCC) can be used for modems during dynamic upstream load balancing.
Step 11	**docsis-policy** *policy-id* **Example:** `Router(config-lb-group)# docsis-policy 1`	Assigns a policy to a DOCSIS LBG. • *policy-id*—LBG policy number. The policy number can range from 0 to 4294967295.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating a Load Balancing Policy

This configuration is optional. This section describes how to create a load balancing policy. You must create at least one load balancing rule before the Cisco CMTS can use a load balancing policy.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	• Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-policy** *policy-id* **rule** *rule-id* **Example:** `Router(config)# cable load-balance docsis-policy 2 rule 1`	Creates a load balancing rule with the following parameters: • *policy-id* —DOCSIS policy to be created. • **rule** *rule-id*—Specifies the rule to be used with the DOCSIS policy.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring a Load Balancing Group

This section describes how to configure an LBG. All steps are optional, unless you want to change the default load balancing configuration.

Restriction When assigning cable interfaces to LBGs, be aware of the following restrictions:

- An upstream can belong to only one LBG.
- All downstreams and upstreams in an LBG must share physical connectivity to the same group of CMs. Downstreams can be in a separate LBG than upstreams, but all downstreams or all upstreams that have the same RF physical connectivity must be members of the same LBG. You cannot distribute downstreams or upstreams that share physical connectivity across multiple LBGs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	• Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-group** *docsis-group-id* **Example:** `Router(config)# cable load-balance group 1 index 81`	Configures a DOCSIS LBG on the Cisco CMTS. • *n* —DOCSIS LBG ID. A valid DOCSIS LBG ID ranges from 1 to 2147483647 and does not overlap with the legacy LBG ID.
Step 4	**downstream cable** *slot/subslot/controller* **Example:** `Router(config-lb-group)# downstream cable 7/0/0`	Assigns a primary downstream channel for a fiber node. • *slot*—Cable interface slot. The valid values range from 5 to 8. • *subslot*—Cable interface subslot. The valid value is 0 or 1. • *controller*—Modular-Cable controller number. The valid values range from 0 to 2.
Step 5	**upstream cable** *slot/subslot/port upstream-list* **Example:** `Router(config-lb-group)# upstream cable 7/0/0 0`	Sets upstream channels in a DOCSIS LBG. • **cable** *slot/subslot/port*—Cisco CMTS interface slot, subslot, and port number parameters. ◦ *slot*—Cable interface slot. The valid values range from 5 to 8. ◦ *subslot*—Cable interface subslot. The valid value is 0 or 1.

	Command or Action	Purpose
		◦ *port*—Modular-cable controller number. The valid values range from 0 to 2. • *upstream-list*—Upstream channel list ranging from 0 to 7.
Step 6	**init-tech-list** *grouplist* [**ucc**] **Example:** `Router(config-lb-group)# init-tech-list 1`	Sets the DCC initialization techniques that the Cisco CMTS can use to load balancing CMs. • *grouplist*—DCC initialization technique list. • **ucc**—(Optional) Determines whether UCC can be used for modems during dynamic upstream load balancing.
Step 7	**docsis-policy** *n* **Example:** `Router(config-lb-group)# docsis-policy 1`	Assigns a policy to a DOCSIS LBG. • *n*—LBG policy number. The policy number can range from 0 to 4294967295.
Step 8	**exit** **Example:** `Router(config-lb-group)# exit`	Exits the DOCSIS LBG on the Cisco CMTS.
Step 9	**cable load-balance group** *n* **policy** {**pcmm** | **ugs** | **us-groups-across-ds**} **Example:** `Router(config)# cable load-balance group 10 policy ugs` `Router(config)# cable load-balance group 10 policy pcmm` `Router(config)# cable load-balance group 10 policy us-groups-across-ds`	Sets the load balancing policy. • *n*—Number of the LBG. In Cisco IOS Release 12.2(33)SCE3 and earlier, the valid range is from 1 to 80. In Cisco IOS Release 12.2(33)SCE4 and later releases, the valid range is from 1 to 256. • **pcmm**—Enables balancing of modems with active PCMM service flows. • **ugs**—Enables balancing of modems with active unsolicited grants service (UGS) service flows. • **us-groups-across-ds**—Enables load balancing on upstream groups across the downstream. The downstream group method will be ignored.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying IGMP-Triggered DCC Load Balancing Operations

This section describes how to use certain show commands to verify the configuration and operation of the IGMP-Triggered DCC Load Balancing feature on the Cisco CMTS.

- **show cable load-balance docsis-group** *vdoc*
- **show cable multicast db detail**
- **show cable multicast db** [*cm-mac-address*]

Examples

The following is a sample output of the **show cable load-balance docsis-group vdoc** command:

```
Router# show cable load-balance docsis-group 2 vdoc
Interface            State Group  Util Total      IGMP    CIR    High Low
                           Index       Targeted   Repl    Init   Util CIR
In7/0/0:0 (453 MHz)  up    81     0%   37(m)      12(m)   25(m)  10   10
In7/0/0:1 (459 MHz)  up    81     0%   37(15)     12(10)  25(5)  30   1
In7/0/0:2 (465 MHz)  up    81     0%   37(m)      12(m)   25(m)  20   10
Util: Current Utilization
Total Targeted: # of times the DS was targeted to be used by VDOC LB
                  w or w/o move
              m: # of times the DS was targeted with a move required

IGMP Repl: subset of Total Targeted, # of times it was due to existing
repl
         m: Targeted via IGMP repl w/ a move required
CIR Init: subset of Total Targetd, # of times it was due to new CIR flow
        m: Targeted via CIR w/ a move required
High Util: #of times the DS was rejected w/ a existing replication due
to high
           util. (regardless of CMs exiting DS)
High CIR: #of times the DS was rejected due to low CIR

Router# show cable multicast db bundle 1 230.1.1.1 detail
Interface            Fwd Intfc   group           source          Cause
Bundle1              Mo3/0/0:0   230.1.1.1       N/A             No LB
ETDB received IGMP   ETDB processed IGMP
Jan 30 03:57:24.759   Jan 30 03:57:24.763
Sid      gc_id    Stat Index   DSID       Stat Index Allocated
DEFAULT  N/A      61322        0x4F259    Jan 30 03:57:24.759
8206     1        61323        0x4F259    Jan 30 03:57:24.759
```

The table below displays the conditions when a new replication is created.

Table 34: Conditions When a New Replication is Created

Cause	Description
NEW_REPLN_NO_LB	Load balancing is not configured.
NEW_REPLN	New replication.
NEW_REPLN_DS_HI_UTIL	Downstream has high utilization of bandwidth.
NEW_REPLN_NO_MOVE	CM move is not allowed.
NEW_REPLN_DS_NOT_LBG	Downstream is not part of the LBG.

Cause	Description
NEW_W_EXIST_REPLN_FOR_WB	Replication exists for the wideband CM.
REPLN_FAIL	Replication failure; use existing replication.
REPLN_DCC	CM requested a DCC.
REPLN_DCC_FAIL	DCC of the CM failure.
REPLN_MDF_DIS	CM was MDF disabled.
REPLN_STATIC_CLI	Static CLI configured.
REPLN_STATIC_TLV	Static TLV configured.
REPLN_INTFC_GC	Interface GC configured.
REPLN_PCMM	PCMM replication.
REPLN_HA	Replication created after HA.

```
Router# show cable multicast db 001e.6bfb.248a
Session (S,G) : (*,230.1.1.1)
Fwd Intfc  Sub Intfc            Host Intfc      Hosts      Proxy    Static   DCC
Mo3/0/0:5  Bundle1              Cable7/0/0          1          N         N     N
```

Additional References

Related Documents

Document Title	URL
Cisco IOS Commands for the Cisco CMTS Routers	http://www.cisco.com/en/US/docs/ios/cable/command/reference/ cbl_book.html
Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC	http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ 12_2sc/cbl_12_2sc_book.html
Cisco uBR10000 Series Universal Broadband Router Release Notes	http://www.cisco.com/en/US/products/hw/cable/ps2209/ prod_release_notes_list.html

Standards and RFCs

Standard/RFC	Title
CableLabs™ DOCSIS specifications	http://www.cablelabs.com/cablemodem/

Standard/RFC	Title
CableLabs™ PacketCable MultiMedia specifications	http://www.cablelabs.com/packetcable/specifications/multimedia.html

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

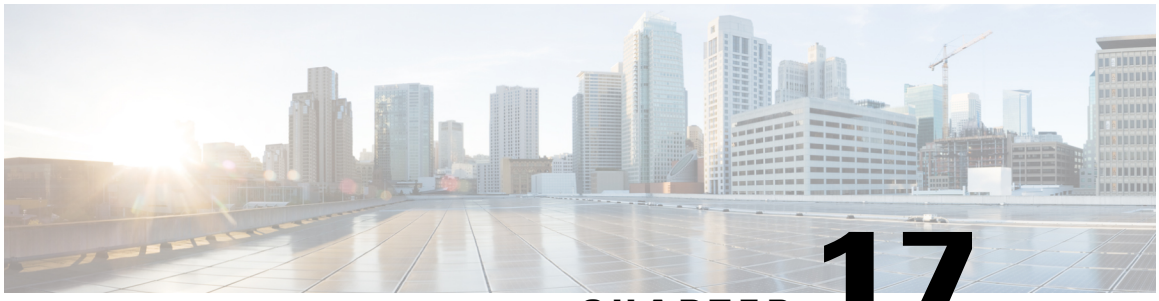
Feature Information for IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 35: Feature Information for IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 CMs

Feature Name	Releases	Feature Information
IGMP-Triggered DCC Load Balancing for DOCSIS 2.0 Cable Modems	12.2(33)SCF	This feature was introduced. The **vdoc** keyword was added to the following commands: • **show cable load-balance vdoc** • **show cable load-balance docsis-group vdoc**



CHAPTER 17

IGMP-Triggered VDOC Broadcast Support on the Cisco CMTS Routers

First Published: December 17, 2008

Last Updated: May 27, 2013

The Cisco universal broadband router supports the Video over DOCSIS (VDOC) Broadcast feature enabling multiple service operators (MSOs) to broadcast video content on RF-spanned downstream signals.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring VDOC Broadcast

The table below shows the hardware compatibility prerequisites for the VDOC broadcast feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 36: Cable Hardware Compatibility Matrix for the VDOC Broadcast Feature

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [24]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [25]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

[24] Cisco uBR3GX60V cable interface line card is compatible only with PRE4.
[25] Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

- The Cisco uBR10012 router must have the M-CMTS setup.
- The Cable Modem Termination System (CMTS) and the cable modem must have the latest DOCSIS 3.0 setup with the Multicast DSID-based Forwarding (MDF) and Dynamic Bonding Change (DBC) capability.
- The cable modem software must support the channel change capability via Receive Channel Configuration (RCC) TLV (49.5) in the DBC message.
- Support for DOCSIS 3.0 channel bonding.

Restrictions for Configuring VDOC Broadcast

- The VDOC Broadcast feature supports:
  - Only one tuner per cable modem.
  - Only one video stream per IP set-top box.
  - Only one IP set-top box for every cable modem.
- Internet Group Management Protocol version 3 (IGMPv3) configuration is required on the bundle interface.
- Secondary bonding groups used for video streams must be created using one or more downstream RF channels.
- The secondary bonding group must not be used for forwarding by other features, such as video on demand (VOD) and service flow attribute-based forwarding interface selection.
- The DPC3010 cable modem (DPC3010 firmware version) might experience 3 seconds delay if receive channel configuration is changed using Dynamic Bonding Change (DBC).

Information About Configuring VDOC Broadcast

The VDOC Broadcast feature facilitates broadcasting video over DOCSIS. Video streams are broadcast to one or more downstream RF channels using static multicast. Depending on the video stream selected for viewing by the IP set-top box, the multituner cable modem is tuned to the appropriate RF channel carrying the specific video stream.

The process to broadcast video over the cable is as follows:

1. When a channel is selected, the IP set-top box sends an IGMP join message to a particular bonding group.
2. The CMTS locates the secondary bonding group that has the video streaming channel and the RCC template that contains the channel corresponding to the secondary bonding group.
3. The CMTS sends a dynamic bonding change request (DBC-REQ) message to the modem. The DBC-REQ message contains the DSID. It also contains a new RCC (that contains frequencies for the primary bonding group and the secondary bonding group that was selected in Step 2), if the modem is not currently tuned to the frequencies selected in Step 2.
4. The cable modem retunes to the new channel and receives the video stream.

Note In the case of subsequent channel changes, the IP set-top box sends an IGMP leave message for the old video stream. CMTS responds with the DBC-REQ message to remove the DSID corresponding to this stream.

Inter Line Card RF Spanning

The Inter Line Card RF Spanning feature, introduced in Cisco IOS Release 12.2(33)SCF, supports sharing of downstream channels across line cards installed on the Cisco uBR10012 router. This feature is an extension to the existing downstream channel sharing functionality supported within the bonding groups configured on a single line card. This feature enables you to associate downstream channels of a line card to a service group that is hosted on a different line card.

Note The Inter Line Card RF Spanning feature is supported only on the Cisco uBR10012 router with Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V cable interface line cards.

The Inter Line Card RF Spanning feature supports the following two methods of downstream channel sharing:

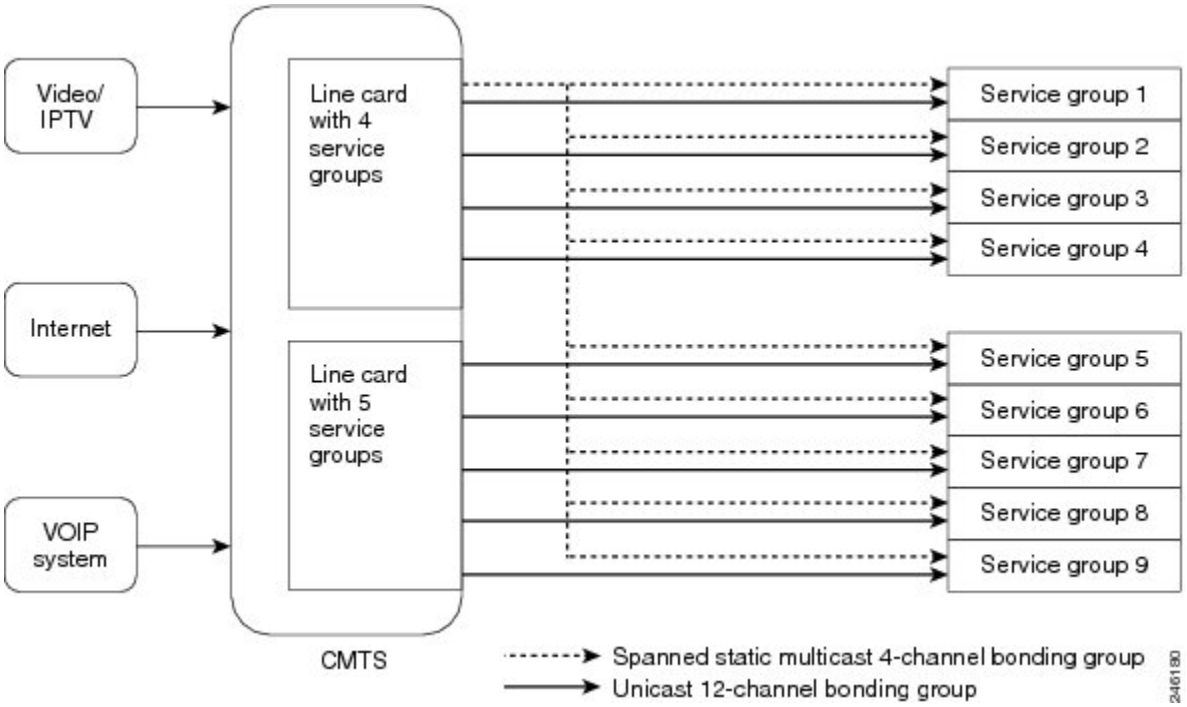
RF Spanning of Bonding Groups Carrying Static Multicast Traffic

In this RF spanning (unrestricted RF spanning) method, a downstream bonding group is configured on one of the line cards and included in one or more fiber nodes as required. Then, one or more static multicast sessions are configured for the bonding group, and any service group can use this bonding group. When this is configured, a cable modem can send a multicast join request and receive multicast streams using this bonding group. This enables service providers to broadcast a set of popular channels and make them available to customers at any time.

As shown in the figure below, each service group is made of 16 downstream channels. Of these 16 channels, 12 downstream channels are from the local card and can carry unicast traffic. The remaining four channels are from one of the line cards and spanned to all downstream service groups. These four channels can carry multicast traffic so that all service groups can use the same channels without creating any replication.

The figure below illustrates how a bonding group carries static multicast traffic.

Figure 3: RF Spanning of Bonding Groups Carrying Static Multicast Traffic



RF Spanning of Remote Bonding Groups

In the RF spanning of remote bonding groups method, downstream channels physically located on a single line card can be used by MAC domains of a different line card for VDOC services. This method supports both unicast VDOC services and static unencrypted multicast services over RF spanned downstream bonding groups. This is similar to the RF spanning functionality supported on the shared port adapter (SPA) bonding groups together with the Cisco uBR10-MC5X20 line card. With this extended RF spanning functionality, you can directly configure remote bonding groups on the Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards for unicast VDOC services. Bonding groups configured on a remote line card are called remote bonding groups.

Note We recommend using a remote bonding group and its associated channels on a single line card only to avoid bandwidth fragmentation and non-deterministic bandwidth allocation behavior.

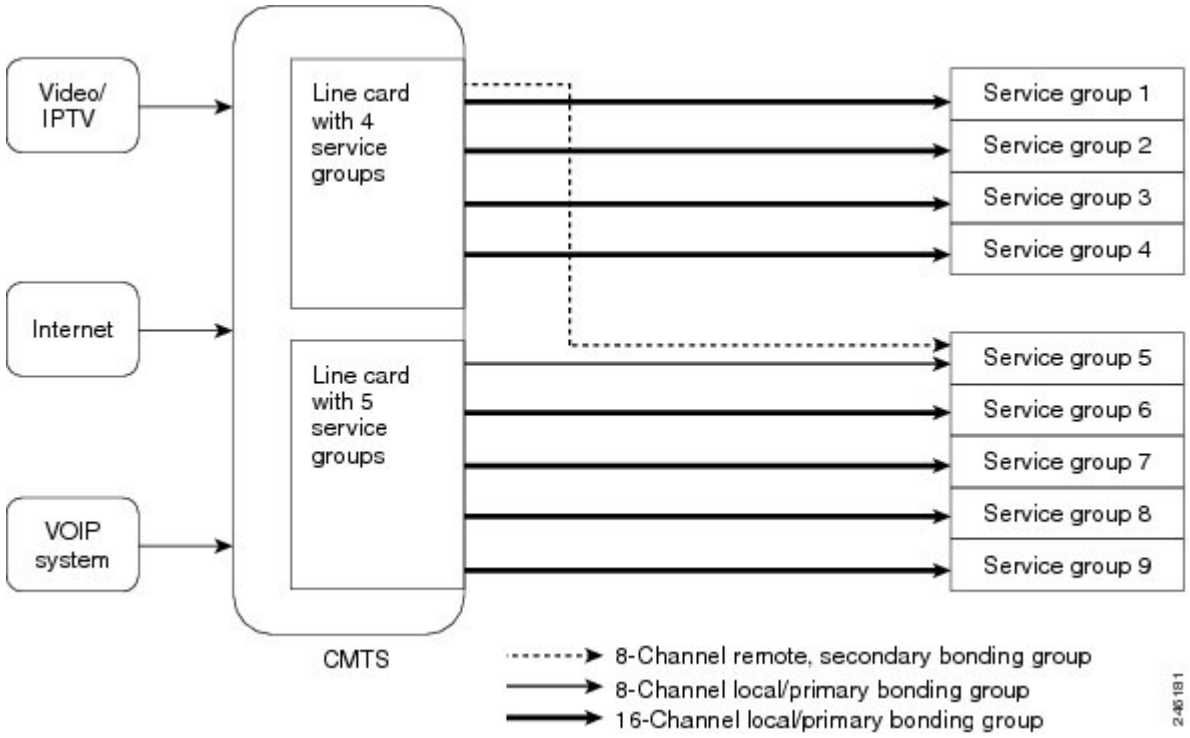
RF spanning of remote bonding groups is configured in the following ways:

Remote Downstream to a Single Host Line Card

As shown in the figure below, each service group is made of 16 downstream channels. Because the Cisco uBR-MC3GX60V line card supports 72 downstream channels, a single line card is not sufficient to make five service groups. Therefore eight downstream channels are taken from another Cisco uBR-MC3GX60V line card to configure five service groups. Also, the service group is made of two or more bonding groups as downstream channels cannot be bonded across line cards.

The figure below illustrates how remote downstream works with a single host line card.

Figure 4: Remote Downstream to a Single Host Line Card



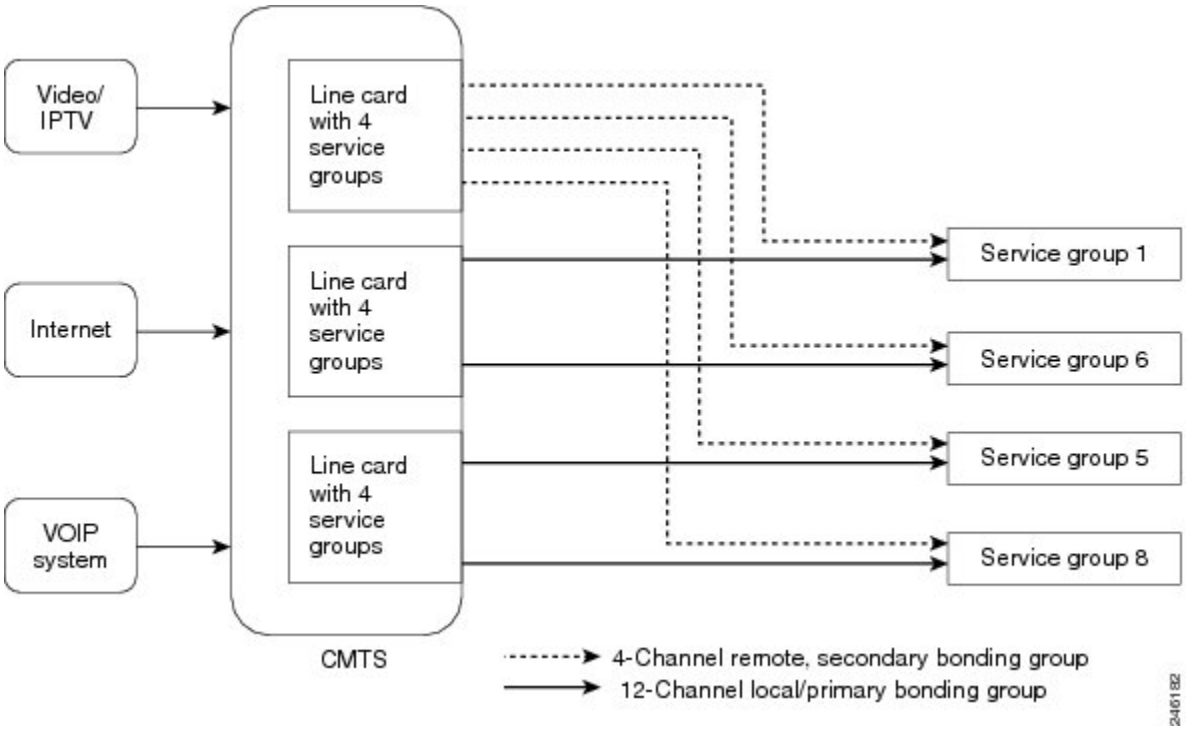
Remote Downstream to Multiple Line Cards

In this configuration, a Cisco uBR-MC3GX60V line card provides all its downstream channels to other Cisco uBR-MC3GX60V line cards installed on the Cisco uBR10012 router. As shown in the figure below, some of the downstream channels are shared with one line card and others are shared with another line card, and none are used locally.

Note This type of configuration may not be efficient even though it is supported to provide flexibility.

The figure below illustrates how remote downstream works with multiple line cards.

Figure 5: Remote Downstream to Multiple Line Cards



This feature also supports mixing of different types of line cards for downstream channel sharing. That is, a MAC domain configured on a Cisco UBR-MC20X20V line card can use a wideband interface configured on a Cisco uBR-MC3GX60V line card and vice versa. However, this type of configuration is generally not required and is not recommended.

RCC Template

This section describes about the RCC template selection:

Dynamic RCC Selection

The dynamic RCC selection feature facilitates multicast forwarding. The RCC selection occurs after the multicast forwarding selection algorithm identifies that the stream being requested is related to the VDOC Broadcast feature. It will select the RCC, which is superset of the primary bonding group of the cable modem, and the secondary bonding group where the stream is forwarded.

Note The RCC template is selected only if the number of RF channels in the primary bonding group of the RCC template is same as the number of RF channels in the primary bonding group of the cable modem currently used.

RCC Assignment Across SPAs

The VDOC Broadcast feature requires modems to be tuned to RF spanned channels carrying video streams. The RF spanned channels originate from a SPA other than the SPA hosting the primary bonding group assigned to the cable modem. RCCs are generated from RCC templates that contain Receive Channels (RC) from multiple SPAs.

Limitations while assigning RCCs are:

- For static multicast streams, only SPA downstream channels can be used in RCC templates.
- Encrypted multicast or unicast traffic is not supported on the RC from a secondary SPA.
- For encrypted or unicast downstream VDOC broadcast, traffic will not be forwarded to CPEs even when the cable modem is properly tuned to the downstream.

How to Configure VDOC Broadcast

This section describes the configuration tasks that are performed when using the VDOC broadcast feature on the Cisco CMTS platform.

1 Configuring the Primary and Secondary Bonding Group, on page 384 (required)
2 Configuring the RCC Template, on page 385 (required)
3 Configuring the Multicast Static Group, on page 387 (required)

Configuring the Primary and Secondary Bonding Group

This section describes the tasks required to configure the MAC domain and the bonding group. Follow the summary steps to complete the configuration.

Configure the modular cable controller for four RF channels, two of which will be used for primary bonding group and the other two will be used for broadcasting video specific bonding groups.

Secondary bonding groups may be constructed using multiple RF channels.

Before You Begin

- The modular controller is already configured for RF channels used for the primary and secondary bonding groups. The RF channels used for secondary bonding groups are non-primary capable and can be served by legacy Edge Quadrature Amplitude Modulation (EQAM) applications. The "udp-port" option can be used instead of Downstream External PHY Interface (DEPI) remote ID.
- The MAC domain is configured by specifying the fiber node configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** *slot/subslot/port:wideband-channel* **Example:** `Router(config)# interface wideband-cable 6/0/1:22`	Enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for the Cisco Wideband SIP. The valid range for a cable line card is from 5 to 8. • *subslot*—Subslot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, subslot 0 is always specified for the Cisco Wideband SIP. For a cable line card, subslot is 0 or 1. • *port*—Bay in the SIP where the Cisco Wideband SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). It also refers to the downstream port of the line card. The valid range varies depending on the line card. • *wideband-channel*—Wideband channel number. The valid range varies depending on the Cisco CMTS router and the line card.
Step 4	**cable bonding-group-secondary** **Example:** `Router(config-if)# cable bonding-group-secondary`	Specifies a secondary bonding group. **Note** The **cable bonding-group-secondary** command replaced the **cable bonding-group-id** command in Cisco IOS Release 12.2(33)SCE.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the RCC Template

This section describes the tasks required to configure the RCC template and associate it to a MAC domain.

RCC templates must be configured and then applied to the MAC domain interface. With 3-channel cable modems, the first two channels are part of the primary bonding group, and the third channel is used for video. If two RF channels are used for carrying video streams, then two RCC templates must be configured.

Before You Begin

Modular controller and MAC domain configuration must be complete before you proceed to configuring the RCC template.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index*} **Example:** `Router(config)# interface cable 8/0/0`	Associates the RCC template to a MAC domain. Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the line card resides. The valid range is from 5 to 8 on the Cisco uBR10012 router. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. The valid subslots are 0 or 1. • *port*—Downstream port number. The valid range is from 0 to 4 (depending on the cable interface) on the Cisco uBR10012 router. • *cable-interface-index*—Downstream port of the Cisco uBR10-MC5X20 and Cisco uBR-MC28 line cards, or MAC domain index of the Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards. The valid range for the Cisco UBR-MC20X20V and Cisco uBR-MC5X20 line cards is from 0 to 4. The valid range for the Cisco uBR-MC3GX60V line card is from 0 to 14.
Step 4	**cable rcc-template** *index* **Example:** `Router(config)# cable rcc-template 1`	Defines the RCC template for a Receive Channel Profile (RCP) outside the MAC domain configuration mode. • *index*—RCC index value. The valid range is from 1 to 255.
Step 5	**rcp-id** *rcp-id* **Example:** `Router(config-rcc-template)# rcp-id 0010000004`	Configures the RCP ID. • *rcp-id*— RCP ID.
Step 6	**receive-module** *index* **first-channel-center-frequency** *Hz* **Example:** `Router(config-rcc-template)# receive-module 1 first-channel-center-frequency 453000000`	Configures the receive module. • *Hz*—Assigned center frequency of the first channel of the receive module channel block in hertz.

	Command or Action	Purpose
Step 7	**receive-channel** *index* **center-frequency** *Hz* **connected-receive-module** *index* [**primary**] **Example:** `Router(config-rcc-template)# receive-channel 1 center-frequency 453000000 connected-receive-module 1 primary`	Configures the receive channel. • *Hz*—Center frequency of a receive channel in Hz. • **connected-receive-module** *index*—Specifies the index value for the connected receive module. The valid range is from 1 to 10. The configuration will be rejected if the connected receive module has not been previously configured. • **primary**— (Optional) Indicates an RCC can be derived with this channel designated as the primary channel of the cable modem.
Step 8	**end** **Example:** `Router(config-rcc-template)# end`	Exits RCC template configuration mode and returns to privileged EXEC mode.

What to Do Next

Note Run the **show cable mac-domain cable interface rcc** command to verify that RCC templates are applied to the MAC domain.

Configuring the Multicast Static Group

Multicast static group configuration is used to statically forward (broadcast) video streams on secondary bonding groups. This configuration specifies certain video streams should be broadcast on particular bonding groups.

This section describes the tasks required to configure the multicast static group.

One or more IGMP static groups corresponding to the broadcast video channels are configured on the specified secondary bonding group. The same groups should be specified under the cable bundle interface as part of the ip igmp static-group command.

Before You Begin

- Multicast routing must be configured on the Cisco CMTS.
- PIM sparse-mode must be configured on the bundle interface.
- IGMPv3 must be configured on the bundle interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *bundle-number* **Example:** `Router# interface bundle 1`	Indicates the bundle interface.
Step 4	**interface wideband-cable** *slot/subslot/port:wideband-channel* **Example:** `Router(config)# interface wideband-cable 6/0/1:22`	Enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for the Cisco Wideband SIP. The valid range for a cable line card is from 5 to 8. • *subslot*—Subslot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, subslot 0 is always specified for the Cisco Wideband SIP. For a cable line card, subslot is 0 or 1. • *port*—Bay in the SIP where the Cisco Wideband SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). It also refers to the downstream port of the line card. The valid range varies depending on the line card. • *wideband-channel*—Wideband channel number. The valid range varies depending on the Cisco CMTS router and the line card.
Step 5	**cable igmp static-group** [*multicast group*] **source** [*source IP*] [*subinterface number*] **Example:** `Router(config-if)# cable igmp static-group 224.0.0.0`	Configures the cable per physical downstream static multicast support on the Cisco CMTS. • *multicast group*—Multicast IP address of the group. • **source** [*source IP*]— (Optional) Source IP address for SSM. • *subinterface number*—Subinterface number. The default is 0 for the main interface. **Note** If the subinterface is configured at the virtual bundle interface, the subinterface number option must be configured to match up with the desired subinterface devices.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

How to Configure Inter Line Card RF Spanning

The following tasks describe how to configure RF spanning of bonding groups carrying static multicast traffic and RF spanning of remote bonding groups to enable RF spanning on the line cards on the Cisco uBR10012 router:

Configuring RF Spanning of Bonding Groups Carrying Static Multicast Traffic

To configure RF spanning of bonding groups carrying static multicast traffic, you need to associate downstream channels to one or more fiber nodes after configuring VDOC features on the Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards.

Before You Begin

- An RCC template must be created and associated to a MAC domain. For details, see Configuring the RCC Template, on page 385
- A multicast static group must be created. For details, see Configuring the Multicast Static Group, on page 387.

Restriction RF spanning of bonding groups carrying static multicast traffic is supported only with static, unencrypted multicast.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable fiber-node** *fiber-node-id*	Enters fiber node configuration mode.

	Command or Action	Purpose
	Example: `Router (config)# cable fiber-node 70`	• *fiber-node-id*—Unique numerical ID of the fiber node. The valid range is from 1 to 256.
Step 4	**downstream modular-cable** *slot/subslot/controller* **rf-channel** *grouplist* **Example:** `Router(config-fiber-node)# downstream modular-cable 6/1/0 rf-channel 7`	Associates the downstream channels to the fiber node of the cable interface line card. • *slot*—Cable interface line card slot. The valid values range from 5 to 8. • *subslot*—Cable interface line card subslot. The valid values are 0 and 1. • *controller*—Cable interface number. The valid range is from 0 to 2. • *grouplist*—Group of RF channels. The valid range is from 0 to 23.
Step 5	**upstream cable** *slot/subslot* **connector** *grouplist* **Example:** `Router(config-fiber-node)# upstream Cable 6/1 connector 3`	Specifies the upstream channel ports for the fiber node. • *slot*—Cable interface line card slot. The valid values range from 5 to 8. • *subslot*—Cable interface line card subslot. The valid values are 0 and 1. • connector—Specifies the physical upstream port connector on the cable interface line card. • *grouplist*—Range of physical port numbers on the cable interface line card. The grouplist can be one or more port numbers, or a range of port numbers separated by a hyphen or combinations of both. The valid range for port numbers is from 0 to 19.
Step 6	**end** **Example:** `Router(config-fiber-node)# end`	Exits fiber node configuration mode and returns to privileged EXEC mode.

Configuring RF Spanning of Remote Bonding Groups

To configure RF spanning of remote bonding groups, you need to configure a wideband interface on the Cisco uBR10012 router.

Before You Begin

- An RCC template must be created and associated to a MAC domain. For details, see Configuring the RCC Template, on page 385
- RF channels must be associated to a fiber node. For details, see Configuring RF Spanning of Bonding Groups Carrying Static Multicast Traffic , on page 389.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** *slot/subslot/port:wideband-channel* **Example:** `Router(config)# interface wideband-cable 6/0/1:22`	Enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for the Cisco Wideband SIP. The valid range for a cable line card is from 5 to 8. • *subslot*—Subslot where the Cisco Wideband SIP or a cable line card resides. On the Cisco uBR10012 router, subslot 0 is always specified for the Cisco Wideband SIP. For a cable line card, subslot is 0 or 1. • *port*—Bay in the SIP where the Cisco Wideband SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). It also refers to the downstream port of the line card. The valid range varies depending on the line card. • *wideband-channel*—Wideband channel number. The valid range varies depending on the Cisco CMTS router and the line card.
Step 4	**cable bundle** *bundle-id* **Example:** `Router(config-if)# cable bundle 1`	Configures the wideband cable interface to belong to an interface bundle. • *bundle-id*—Bundle identifier. The valid range is from 1 to 255.
Step 5	**cable rf-channel** *rf-channel* **bandwidth-percent** *bw-percent* **Example:** `Router(config-if)# cable rf-channel 0 bandwidth-percent 25`	Configures the bandwidth of the RF channel that would be allocated to a specified wideband channel or bonding group. • *rf-channel*—RF channel on the physical port of the field-programmable gate array (FPGA). • **bandwidth-percent** *bw-percent*—(Optional) Indicates the percentage of bandwidth from this RF channel that is used for the wideband interface. The valid range is from 0 to 100 percent. The default bandwidth value is 100.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for VDOC Broadcast

This section describes a sample configuration example for configuring the VDOC broadcast feature.

This configuration supports four video channels (IGMP groups) over two bonding groups, with two channels over one bonding group each. Depending on the video channel selected by the set-top box, the cable modem tunes to frequencies in either RCC template 1 or 2.

Example: Configuring the Primary and Secondary Bonding Groups

The following example shows how to configure the primary and secondary bonding groups. This example is valid for Cisco IOS Release 12.2(33)SCD and earlier.

Note Secondary bonding group configuration is required only for the VDOC Broadcast feature. This configuration is not required for Inter Line Card RF Spanning.

```
controller modular-cable 1/0/0
 ip-address 192.0.2.0
 modular-host subslot 6/0
 rf-channel 0 cable downstream channel-id 24
 rf-channel 0 frequency 453000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 20000
 rf-channel 1 cable downstream channel-id 25
 rf-channel 1 frequency 459000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21000
 rf-channel 2 cable downstream channel-id 26
 rf-channel 2 frequency 465000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21001
 rf-channel 3 cable downstream channel-id 27
 rf-channel 3 frequency 471000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21002
!
Router(config)# interface Wideband-Cable1/0/0:0
cable bundle 1
 cable bonding-group-id 1

0 bandwidth-percent 80
 cable rf-channel 1
!
Router(config)# interface Wideband-Cable1/0/0:1
 cable bundle 1
 cable bonding-group-id 2 secondary
 cable rf-channel 2
!
Router(config)# interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3 secondary
 cable rf-channel 3
!
Router(config)# interface Modular-Cable1/0/0:0
 cable bundle 1
 cable rf-bandwidth-percent 10
!
cable fiber-node 1
 downstream Modular-Cable 1/0/0 rf-channel 0-3
!
```

The following example shows how to configure secondary bonding groups in Cisco IOS Release 12.2(33)SCE and later.

```
controller modular-cable 1/0/0
 ip-address 192.0.2.0
 modular-host subslot 6/0
 rf-channel 0 cable downstream channel-id 24
 rf-channel 0 frequency 453000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 20000
 rf-channel 1 cable downstream channel-id 25
 rf-channel 1 frequency 459000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21000
 rf-channel 2 cable downstream channel-id 26
 rf-channel 2 frequency 465000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21001
 rf-channel 3 cable downstream channel-id 27
 rf-channel 3 frequency 471000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 192.0.2.0 mac-address 0090.f001.930c depi-remote-id 21002
!
Router(config)# interface Wideband-Cable1/0/0:0
cable bundle 1
cable bonding-group-secondary
cable rf-channel 0 bandwidth-percent 80 cable rf-channel 1
!
Router(config)# interface Wideband-Cable1/0/0:1
cable bundle 1
cable bonding-group-secondary
cable rf-channel 2
!
Router(config)# interface Wideband-Cable1/0/0:2
cable bundle 1
cable bonding-group-secondary
cable rf-channel 3
!
Router(config)# interface Modular-Cable1/0/0:0
 cable bundle 1
 cable rf-bandwidth-percent 10
!
cable fiber-node 1
 downstream Modular-Cable 1/0/0 rf-channel 0-3
!
```

Example: Configuring the RCC Template

The following example shows how to apply RCC templates to the MAC domain host interface. The frequencies used to configure the MAC domain and bonding group are also used here.

```
cable rcc-template 1
  rcp-id 00 10 18 33 81
  receive-module 1 first-center-frequency 453000000
  receive-channel 1 center-frequency 453000000 connected-receive-module 1 primary
  receive-channel 2 center-frequency 459000000 connected-receive-module 1
  receive-channel 3 center-frequency 465000000 connected-receive-module 1
!
cable rcc-template 2
rcp-id 00 10 18 80 61
  receive-module 1 first-center-frequency 465000000
  receive-module 2 first-center-frequency 489000000
  receive-channel 1 center-frequency 465000000 connected-receive-module 1 primary
  receive-channel 2 center-frequency 471000000 connected-receive-module 1
  receive-channel 3 center-frequency 477000000 connected-receive-module 1
  receive-channel 4 center-frequency 483000000 connected-receive-module 1
  receive-channel 5 center-frequency 489000000 connected-receive-module 2
  receive-channel 6 center-frequency 495000000 connected-receive-module 2
  receive-channel 7 center-frequency 501000000 connected-receive-module 2
  receive-channel 8 center-frequency 507000000 connected-receive-module 2
!
interface Cable 6/0/0
```

```
 downstream Modular-Cable 1/0/0 rf-channel 0 upstream 0-3
cable rcc-template 1
cable rcc-template 2
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 119
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 615000000
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
```

Example: Configuring the Multicast Static Group

The following example shows how to configure multicast static groups on the bundle interface and on bonding groups in Cisco IOS Release 12.2(33)SCD and earlier:

```
interface Bundle 1
 ip address 192.0.2.8 255.255.255.0
 ip pim sparse-mode
 ip helper-address 2.39.16.1
 ip igmp static-group 224.0.2.1
 ip igmp static-group 224.0.2.2
 ip igmp static-group 224.0.2.3
 ip igmp static-group 224.0.2.4
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
!
Router(config)# interface Wideband-Cable1/0/0:1
 cable bundle 1
Router(config)#cable igmp static-group 224.0.2.3
Router(config)#cable igmp static-group 224.0.2.4
 cable bonding-group-id 2 secondary
 cable rf-channel 2
!
Router(config)#interface Wideband-Cable1/0/0:2
 cable bundle 1
Router(config)#cable igmp static-group 224.0.2.1
```

```
Router(config)#cable igmp static-group 224.0.2.2
 cable bonding-group-id 3 secondary
 cable rf-channel 3
```

The following example shows how to configure multicast static groups on the bundle interface and on bonding groups in Cisco IOS Release 12.2(33)SCE and later:

```
interface Bundle 1
 ip address 192.0.2.8 255.255.255.0
 ip pim sparse-mode
 ip helper-address 2.39.16.1
 ip igmp static-group 224.0.2.1
 ip igmp static-group 224.0.2.2
 ip igmp static-group 224.0.2.3
 ip igmp static-group 224.0.2.4
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
!
Router(config)# interface Wideband-Cable1/0/0:1
 cable bundle 1
Router(config)#cable igmp static-group 224.0.2.3
Router(config)#cable igmp static-group 224.0.2.4
 cable bonding-group-secondary
 cable rf-channel 2
!
Router(config)#interface Wideband-Cable1/0/0:2
 cable bundle 1
Router(config)#cable igmp static-group 224.0.2.1
Router(config)#cable igmp static-group 224.0.2.2
 cable bonding-group-secondary 3
 cable rf-channel 3
```

Configuration Examples for Inter Line Card RF Spanning

This section provides configuration examples for the Inter Line Card RF Spanning feature.

Example: RF Spanning of Bonding Groups Carrying Static Multicast Traffic

The following example shows how to configure RF spanning of bonding groups carrying static multicast traffic on the Cisco uBR100 router:

```
controller Modular-Cable 1/2/0
 modular-host subslot 7/0
 rf-channel 0 cable downstream channel-id 193
 rf-channel 0 frequency 549000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500025
 rf-channel 1 cable downstream channel-id 194
 rf-channel 1 frequency 555000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500026
 rf-channel 2 cable downstream channel-id 195
 rf-channel 2 frequency 561000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500027
 rf-channel 3 cable downstream channel-id 196
 rf-channel 3 frequency 567000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500028

interface Wideband-Cable1/2/0:0
 cable bundle 11
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
controller Modular-Cable 5/0/0
 ip-address 60.3.2.4
 rf-channel 0 cable downstream channel-id 5
```

```
 rf-channel 0 frequency 501000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500017
 rf-channel 1 cable downstream channel-id 1
 rf-channel 1 frequency 507000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500018
 rf-channel 2 cable downstream channel-id 2
 rf-channel 2 frequency 513000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500019
 rf-channel 3 cable downstream channel-id 3
 rf-channel 3 frequency 519000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500020

interface Wideband-Cable5/0/0:0
 cable bundle 11
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10

controller Modular-Cable 6/0/0
 ip-address 60.3.2.3
 rf-channel 0 cable downstream channel-id 4
 rf-channel 0 frequency 405000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500001
 rf-channel 1 cable downstream channel-id 22
 rf-channel 1 frequency 411000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500002
 rf-channel 2 cable downstream channel-id 23
 rf-channel 2 frequency 417000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500003
 rf-channel 3 cable downstream channel-id 24
 rf-channel 3 frequency 423000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500004
interface Wideband-Cable6/0/0:0
 cable bundle 11
 cable igmp static-group 230.1.1.1 1
 cable igmp static-group 230.5.5.5 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
cable fiber-node 50
 downstream Modular-Cable 5/0/0 rf-channel 0-3
 downstream Modular-Cable 6/0/0 rf-channel 0-3
 upstream Cable 5/0 connector 0-3
cable fiber-node 70
 downstream Modular-Cable 1/2/0 rf-channel 0-3
 downstream Modular-Cable 6/0/0 rf-channel 0-3
 upstream Cable 7/0 connector 0-3
```

Example: RF Spanning of Remote Bonding Groups

The following example shows how to configure RF spanning of remote bonding groups on the Cisco uBR100 router:

```
controller Modular-Cable 5/0/0
 ip-address 60.3.2.4
 rf-channel 0 cable downstream channel-id 5
 rf-channel 0 frequency 501000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500017
 rf-channel 1 cable downstream channel-id 1
 rf-channel 1 frequency 507000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500018
 rf-channel 2 cable downstream channel-id 2
 rf-channel 2 frequency 513000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500019
 rf-channel 3 cable downstream channel-id 3
 rf-channel 3 frequency 519000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500020
```

```
interface Wideband-Cable5/0/0:0
 cable bundle 11
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10

controller Modular-Cable 6/0/0
 ip-address 60.3.2.3
 rf-channel 0 cable downstream channel-id 4
 rf-channel 0 frequency 405000000 annex B modulation 256qam interleave 32
 rf-channel 0 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500001
 rf-channel 1 cable downstream channel-id 22
 rf-channel 1 frequency 411000000 annex B modulation 256qam interleave 32
 rf-channel 1 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500002
 rf-channel 2 cable downstream channel-id 23
 rf-channel 2 frequency 417000000 annex B modulation 256qam interleave 32
 rf-channel 2 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500003
 rf-channel 3 cable downstream channel-id 24
 rf-channel 3 frequency 423000000 annex B modulation 256qam interleave 32
 rf-channel 3 ip-address 60.3.2.1 mac-address 0022.9084.8d7f depi-remote-id 500004
interface Wideband-Cable6/0/0:0
 cable bundle 11
 cable igmp static-group 230.1.1.1 1
 cable igmp static-group 230.5.5.5 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable rf-channel 3 bandwidth-percent 10
cable fiber-node 50
 downstream Modular-Cable 5/0/0 rf-channel 0-3
 downstream Modular-Cable 6/0/0 rf-channel 0-3
 upstream Cable 5/0 connector 0-3
```

Verifying VDOC Broadcast and Inter Line Card RF Spanning

To verify configuration of VDOC broadcast and inter line card RF spanning, use the following commands:

- **show controller integrated-cable**
- **show controller modular-cable**
- **show cable multicast db**
- **show cable mac-domain rcc**
- **show cable modem service-flow**
- **show cable active-reman**

To verify that the bonding group being shared by service groups is associated with all relevant MAC domains of the Cisco UBR-MC20X20V line card, use the **show controller integrated-cable** command with the association keyword as shown in the following example:

```
Router# show controller integrated-cable 8/0/1 association
WB Association Info for 8/0 No of WB 30
WB                    BG   Bundle  NB          NB chan  Reserved  Total
channel               ID   num     channel     ID       CIR       CIR
Wideband-Cable8/0/0:0   1217 11      Cable7/0/0  0        0         6000000
                                     Multicast           0         6000000
Wideband-Cable8/0/0:1   1218 11      Cable7/0/0  0        0         1500000
                                     Multicast           0         1500000
Wideband-Cable8/0/0:2   1219 11      Cable7/0/0  0        0         1500000
                                     Multicast           0         1500000
Wideband-Cable8/0/1:0   1249 11      Cable7/0/0  0        0         6000000
```

```
                                    Multicast           0         6000000
```

To verify that the bonding group being shared by service groups is associated with all relevant MAC domains of the Cisco uBR-MC3GX60V line card, use the **show controller modular-cable** command with the association keyword as shown in the following example:

```
Router# show controller modular-cable 5/0/0 association
WB Association Info for 5/0 No of WB 96
WB                      BG   Bundle  NB          NB chan  Reserved  Total
channel                 ID   num     channel     ID       CIR       CIR
Wideband-Cable5/0/0:0   257  11      Cable5/0/0  0        0         6000000
                                     Multicast           0         6000000
Wideband-Cable5/0/0:1   258  11      Cable5/0/0  0        0         4500000
                                     Multicast           0         4500000
Wideband-Cable5/0/0:2   259  11      Cable5/0/1  0        0         6000000
                                     Multicast           0         6000000
Wideband-Cable5/0/0:3   260  11      Cable5/0/1  0        0         4500000
                                     Multicast           0         4500000
```

To verify the multicast bundle interface, use the **show cable multicast db** command with the bundle keyword as shown in the following example:

```
Router# show cable multicast db bundle 11
Interface : Bundle11.1
Session (S,G) : (*,230.40.40.40)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:4  Bundle11.1           Ca5/0/1      ff05.0000.0024       1
Interface : Bundle11.1
Session (S,G) : (*,230.40.40.40)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:0  Bundle11.1           Ca5/0/0      ff05.0000.0020       1
Interface : Bundle11.1
Session (S,G) : (*,230.40.40.40)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:1  Bundle11.1           Ca7/0/0      ff01.0002.0021       1
Interface : Bundle11.1
Session (S,G) : (*,230.40.40.40)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:0  Bundle11.1           Ca7/0/0      ff01.0002.0020       1
Interface : Bundle11.1
Session (S,G) : (*,230.50.50.50)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:4  Bundle11.1           Ca5/0/1      ff05.0000.0024       1
Interface : Bundle11.1
Session (S,G) : (*,230.50.50.50)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:0  Bundle11.1           Ca5/0/0      ff05.0000.0020       1
Interface : Bundle11.1
Session (S,G) : (*,230.50.50.50)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:1  Bundle11.1           Ca7/0/0      ff01.0002.0021       1
Interface : Bundle11.1
Session (S,G) : (*,230.50.50.50)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:0  Bundle11.1           Ca7/0/0      ff01.0002.0020       1
Interface : Bundle11.1
Session (S,G) : (*,230.7.7.7)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Wi6/0/0:1  Bundle11.1           Ca6/0/0      ff06.0000.0001       1
Interface : Bundle11.1
Session (S,G) : (*,230.5.5.5)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Wi6/0/0:0  Bundle11.1           Ca6/0/0      ff06.0000.0000       1
Interface : Bundle11.1
Session (S,G) : (*,230.2.2.2)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Wi6/0/0:1  Bundle11.1           Ca6/0/0      ff06.0000.0001       1
Interface : Bundle11.1
Session (S,G) : (*,230.1.1.1)
```

```
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Wi6/0/0:0  Bundle11.1           Ca6/0/0      ff06.0000.0000       1
Interface : Bundle11.1
Session (S,G) : (*,230.30.30.30)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:4  Bundle11.1           Ca5/0/1      ff05.0000.0024       1
Interface : Bundle11.1
Session (S,G) : (*,230.30.30.30)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo5/0/0:0  Bundle11.1           Ca5/0/0      ff05.0000.0020       1
Interface : Bundle11.1
Session (S,G) : (*,230.30.30.30)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:1  Bundle11.1           Ca7/0/0      ff01.0002.0021       1
Interface : Bundle11.1
Session (S,G) : (*,230.30.30.30)
Fwd Intfc  Sub Intfc            Host Intfc   CM Mac           Hosts
Mo1/2/0:0  Bundle11.1           Ca7/0/0      ff01.0002.0020       1
```

To verify that the right RCC templates are available for the remote MAC domain, use the **show cable mac-domain rcc** command as shown in the following example:

```
Router# show cable mac-domain cable 5/0/0 rcc
RCC-ID RCP RCs MD-DS-SG CMs WB/RCC-TMPL
1 00 10 00 00 04 4 1 0 RCC-TMPL (1)
2 00 10 00 00 04 4 1 8 RCC-TMPL (2)
3 00 10 00 00 04 8 1 2 RCC-TMPL (5)
4 00 10 00 00 04 8 1 2 RCC-TMPL (6)
5 00 00 00 00 00 4 0 0 WB (Wi5/0/0:0)
6 00 00 00 00 00 3 0 0 WB (Wi5/0/0:1)
7 00 00 00 00 00 2 0 0 WB (Wi5/0/0:4)
8 00 00 00 00 00 1 0 0 WB (Wi5/0/0:5)
9 00 00 00 00 00 1 0 0 WB (Wi5/0/0:6)
10 00 00 00 00 00 1 0 0 WB (Wi5/0/0:7)
11 00 00 00 00 00 1 0 0 WB (Wi5/0/0:8)
12 00 00 00 00 00 2 0 0 WB (Wi5/0/0:9)
13 00 00 00 00 00 4 0 0 WB (Wi6/0/0:1)
14 00 00 00 00 00 1 0 0 WB (Wi6/0/0:2)
15 00 00 00 00 00 1 0 0 WB (Wi6/0/0:3)
16 00 00 00 00 00 3 0 0 WB (Wi6/0/0:6)
17 00 00 00 00 00 3 0 0 WB (Wi6/0/0:7)
18 00 00 00 00 00 2 0 0 WB (Wi6/0/0:8)
```

To verify that the service flows are established correctly on local and remote bonding groups, use the **show cable modem service-flow** command as shown in the following example:

```
Router# show cable modem 0022.ce89.9664 service-flow
SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num Primary
DS
                               Interface     State         Sid   CPE Downstream
RfId
0022.ce89.9664 30.13.2.74      C5/0/0/UB     w-online(pt)  1     0   Mo5/0/0:0
240
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
15    US  act   1     BE     0    0           3044        0           0
16    DS  act   N/A   BE     0    1000012     6000000     0           0
33    DS  act   N/A   BE     0    1000012     6000000     0           0
UPSTREAM SERVICE FLOW DETAIL:
SFID  SID   Requests   Polls      Grants     Delayed    Dropped    Packets
                                             Grants     Grants
15    1     0          0          401        0          0          416
DOWNSTREAM SERVICE FLOW DETAIL:
SFID  RP_SFID QID    Flg Policer              Scheduler             FrwdIF
                         Xmits      Drops      Xmits      Drops
16    33559   132579     51         0          51         0          Wi5/0/0:1
33    33560   132580     0          0          0          0          Wi6/0/0:2
Flags Legend:
$: Low Latency Queue (aggregated)
```

```
~: CIR Queue
```

To verify the line card high availability information for all interfaces, use the **show cable active-reman** command as shown in the following example:

```
Router# show cable active-reman all
------------------------------------------------------------
Active Reman info on LC 5/0:
[slot_index 0]:  work_slot:1/0,  active_slot:1/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 1]:  work_slot:3/0,  active_slot:3/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 2]:  work_slot:5/0,  active_slot:5/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 3]:  work_slot:5/1,  active_slot:5/1,  is_protect:TRUE ,  is_standby
:TRUE
[slot_index 4]:  work_slot:6/0,  active_slot:6/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 5]:  work_slot:6/1,  active_slot:6/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 6]:  work_slot:7/0,  active_slot:7/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 7]:  work_slot:7/1,  active_slot:7/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 8]:  work_slot:8/0,  active_slot:8/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 9]:  work_slot:8/1,  active_slot:8/1,  is_protect:FALSE,  is_standby
:FALSE
------------------------------------------------------------
Active Reman info on LC 5/1:
[slot_index 0]:  work_slot:1/0,  active_slot:1/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 1]:  work_slot:3/0,  active_slot:3/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 2]:  work_slot:5/0,  active_slot:5/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 3]:  work_slot:5/1,  active_slot:5/1,  is_protect:TRUE ,  is_standby
:TRUE
[slot_index 4]:  work_slot:6/0,  active_slot:6/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 5]:  work_slot:6/1,  active_slot:6/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 6]:  work_slot:7/0,  active_slot:7/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 7]:  work_slot:7/1,  active_slot:7/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 8]:  work_slot:8/0,  active_slot:8/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 9]:  work_slot:8/1,  active_slot:8/1,  is_protect:FALSE,  is_standby
:FALSE
------------------------------------------------------------
Active Reman info on LC 6/0:
[slot_index 0]:  work_slot:1/0,  active_slot:1/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 1]:  work_slot:3/0,  active_slot:3/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 2]:  work_slot:5/0,  active_slot:5/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 3]:  work_slot:5/1,  active_slot:5/1,  is_protect:TRUE ,  is_standby
:TRUE
[slot_index 4]:  work_slot:6/0,  active_slot:6/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 5]:  work_slot:6/1,  active_slot:6/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 6]:  work_slot:7/0,  active_slot:7/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 7]:  work_slot:7/1,  active_slot:7/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 8]:  work_slot:8/0,  active_slot:8/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 9]:  work_slot:8/1,  active_slot:8/1,  is_protect:FALSE,  is_standby
```

```
:FALSE
------------------------------------------------------------
Active Reman info on LC 7/0:
[slot_index 0]:  work_slot:1/0,  active_slot:1/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 1]:  work_slot:3/0,  active_slot:3/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 2]:  work_slot:5/0,  active_slot:5/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 3]:  work_slot:5/1,  active_slot:5/1,  is_protect:TRUE ,  is_standby
:TRUE
[slot_index 4]:  work_slot:6/0,  active_slot:6/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 5]:  work_slot:6/1,  active_slot:6/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 6]:  work_slot:7/0,  active_slot:7/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 7]:  work_slot:7/1,  active_slot:7/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 8]:  work_slot:8/0,  active_slot:8/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 9]:  work_slot:8/1,  active_slot:8/1,  is_protect:FALSE,  is_standby
:FALSE
------------------------------------------------------------
Active Reman info on LC 8/0:
[slot_index 0]:  work_slot:1/0,  active_slot:1/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 1]:  work_slot:3/0,  active_slot:3/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 2]:  work_slot:5/0,  active_slot:5/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 3]:  work_slot:5/1,  active_slot:5/1,  is_protect:TRUE ,  is_standby
:TRUE
[slot_index 4]:  work_slot:6/0,  active_slot:6/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 5]:  work_slot:6/1,  active_slot:6/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 6]:  work_slot:7/0,  active_slot:7/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 7]:  work_slot:7/1,  active_slot:7/1,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 8]:  work_slot:8/0,  active_slot:8/0,  is_protect:FALSE,  is_standby
:FALSE
[slot_index 9]:  work_slot:8/1,  active_slot:8/1,  is_protect:FALSE,  is_standby
```

Additional References

The following sections provide references related to configuring the VDOC Broadcast feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Related Topic	Document Title
PacketCable and PacketCable Multimedia	*PacketCable and PacketCable Multimedia for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm.html
DOCSIS 3.0 multicast	DOCSIS 3.0 Multicast Support on the CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_d30_mcast_support.html

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

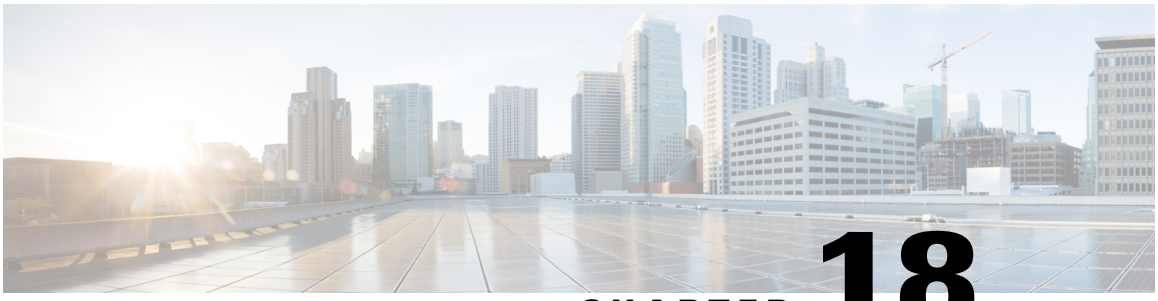
Feature Information for Configuring VDOC Broadcast

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 37: Feature Information for Configuring VDOC Broadcast

Feature Name	Releases	Feature Information
IGMP-Triggered VDOC Broadcast Support	12.2(33)SCB	The Cisco universal broadband router supports VDOC feature enabling MSOs to broadcast video content on RF spanned downstream signals. The following sections provide information about this feature: • Information About Configuring VDOC Broadcast, on page 379 • How to Configure VDOC Broadcast, on page 384 • Configuration Examples for VDOC Broadcast, on page 392 • Verifying VDOC Broadcast and Inter Line Card RF Spanning, on page 397
Inter Line Card RF Spanning	12.2(33)SCF	The Inter Line Card RF Spanning feature supports sharing of downstream channels among the line cards installed on the Cisco uBR10012 router. The following sections provide information about this feature: • Inter Line Card RF Spanning, on page 380 • How to Configure Inter Line Card RF Spanning, on page 389 • Configuration Examples for Inter Line Card RF Spanning , on page 395 The following commands were introduced or modified: • **show cable active-reman** • **show cable multicast db**



CHAPTER 18

Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: October 25, 2013

Load Balancing (LB) for the Cisco CMTS allows system operators to distribute cable modems across radio frequency (RF) downstream (DS) and upstream (US) channels on the same cable interface line card, or across multiple cable interface line cards in some circumstances. Load balancing maximizes bandwidth and usage of the cable plant.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Load balancing supports multiple methods to achieve greater bandwidth availability and performance of the Cisco CMTS with subscriber benefits. These include static and dynamic load balancing schemes, inter-line card and intra-line card support, in some circumstances, configuration of load balancing groups (LBGs) that entail multiple interfaces, multiple load balancing policies, and the option to configure multiple additional load balancing parameters.

The load balancing policies can be configured on the Cisco CMTS, indexed by an ID, to limit the movement of CMs within a Load Balancing Group (LBG). The CM will forward TLV43.1 in its registration request (REG-REQ) message, which is then parsed and stored in the Cisco CMTS. A policy defines whether and when CMs can be moved within their load balancing groups.

During dynamic load balancing, the specified policy of the CM is checked to determine whether the CM is allowed to move. However, existing static load balancing using a frequency override technique and passive load balancing still take action at ranging time.

Effective with Cisco IOS Release 12.3(17a)BC, and later 12.3 BC releases, load balancing is enhanced and supported with Dynamic Channel Change (DCC). DCC in DOCSIS 1.1 dynamically changes cable modem upstream or downstream channels without forcing a cable modem to go offline, and without reregistration after the change.

Effective with Cisco IOS Release 12.3(17b)BC4, and later releases, load balancing is enhanced to distribute downstream load balancing with upstream channel loads in the same upstream load balancing group. This improves upon the prior load balancing limitation, in which load balancing was implemented on the basis of the entire downstream channel load.

Effective with Cisco IOS Release 12.2(33)SCB, and later releases, load balancing is enhanced to use rules and policies to decide on moving the CMs within their LB groups. These policies are created on the Cisco CMTS and chosen on a per-CM basis using type-length-value (TLV) portion (43.1, Policy ID) of REG-REQ. These policies prohibit a modem from being moved or restricted.

A policy contains a set of rules. When the policy is defined by multiple rules, all rules apply in combinations. A rule can be defined as “enabled”, “disabled”, or “disabled during time period.” Each rule can be used by more than one policy.

Effective with Cisco IOS Release 12.2(33)SCF1, DOCSIS 3.0 static modem count-based load balancing is enhanced to use the dynamic bonding change (DBC) to modify the following parameters of DOCSIS 3.0 cable modem with multiple transmit channel (MTC) mode or multiple receive channel (MRC) mode without primary channel change:

- Transmit channel set (TCS)
- Receive channel set (RCS)
- Downstream IDs (DSID) or DSID-associated attributes
- Security association for encrypting downstream traffic

These parameters and additional load balancing schemes are supported on the Cisco CMTS, and described in this document. This document describes all implementations of load balancing on the Cisco CMTS, dependent upon the Cisco IOS release installed and the desired parameters.

Effective with Cisco IOS Release 12.2(33)SCG1, the Cisco uBR-MC3GX60V line card and up to five shared port adapters (SPAs) can be configured to the same LBG. You can:

- Include all the downstreams and upstreams of the SPA cards and the Cisco uBR-MC3GX60V line card in the LBG.
- Configure the MAC domain to include the SPA cards and the Cisco uBR-MC3GX60V line card.
- Configure the fiber-node to include all the downstreams and upstreams of the SPA cards and the Cisco uBR-MC3GX60V line card.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites

The Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change feature is supported on the Cisco CMTS routers in Cisco IOS Releases 12.3BC and 12.2SC. The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS release are supported in all subsequent releases unless otherwise specified.

Table 38: Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2[26] Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[27]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [28]

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

26 PRE = Processor Routing Engine

27 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

28 Cisco uBR-MC88V cable interface line card is only compatible with NPE-G2.

Prerequisites for Load Balancing

The Load Balancing feature has the following prerequisites:

- Load balancing can be done only on upstreams and downstreams that share physical connectivity with the same group of cable modems.
- When performing load balancing among downstreams, you must also configure the known downstream center frequency to be used on each downstream interface, using the **cable downstream frequency** command. (This is an information-only configuration on cable interfaces that use an external upconverter, but it is still required for load balancing so that the Cisco CMTS knows what frequencies it should use when moving cable modems from one downstream to another.)

Prerequisites for Dynamic Channel Change for Load Balancing

- DCC can be done only to a cable modem that is physically connected to both source and target upstream or downstream channels, or both.
- Upstreams and downstream channels that share the same physical connectivity must have different center frequencies separated by channel width.
- The difference between the physical layer parameters on the source and target DCC channels must be within the threshold required by the desired DCC initialization technique.
- DOCSIS 1.1 must be enabled for a modem to behave properly for the DCC operation. Note that not all DOCSIS 1.1 certified modems are DCC-capable, as the CableLabs DCC ATP tests need enhancement for complete coverage.

Prerequisites for Dynamic Bonding Change for DOCSIS 3.0 Static Modem Count-Based Load Balancing

- Initialization techniques 1 to 4, when used, require the Cisco CMTS to include the upstream channel descriptor (UCD) TLV (TLV46.5) in the DBC-REQ message.

- Bandwidth must be sufficient on the target bonding group to support DBC. This is determined by the admission control APIs.
- Fiber nodes must be configured before configuring DOCSIS 3.0 static modem count-based load balancing.

Restrictions

The following sections describe the restrictions applicable for the Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change feature:

Restrictions for Load Balancing

The Load Balancing feature has the following restrictions:

- Load balancing can be done only on a per-chassis basis—all interfaces in a load balancing group must be provided by the same chassis.

  Load balancing can be done only on a per-line card basis—all interfaces in a load balancing group must be provided by the same line card.
- A downstream or upstream can belong to only one load balancing group.
- All downstreams and upstreams in a load balancing group must share physical connectivity to the same group of cable modems. Downstreams can be in a separate load balancing group than upstreams, but all downstreams or all upstreams that have the same RF physical connectivity must be members of the same load balancing group.
- You can configure only one load balancing group per shared physical domain (upstream or interface). You cannot configure multiple load balancing groups to distribute downstreams or upstreams that share physical connectivity.
- You can create a maximum of 80 load balancing groups on each chassis (the older limitation was 20).
- If an upstream port is operational, using the **no shutdown** command, and is not being used and not connected, load balancing attempts to use the port even though there are no cable modems registered on that port. When the upstream port is up, it is put into INIT state and load balancing includes this port as a potential target. However, if the load balancing sees multiple failures moving to this upstream, it is set to DISABLE state and the port is avoided later on in load balancing processes.
- The load balancing algorithms assume a relatively even distribution of usage among modems. In the situation where one cable modem creates the bulk of the load on an interface, the load balancing thresholds should be configured for a value above the load created by that single modem.
- Load balancing is done on cable modems in real time, using current load-usage statistics. You cannot perform load balancing according to the time of day or using a schedule.
- You cannot select particular cable modems to be automatically moved for load balancing, although you can exclude cable modems from load balancing operations altogether on the basis of their MAC address or organization unique identifier (OUI). (You can use the **test cable load-balance** command to manually move a particular cable modem among upstreams, but this is done typically to test the configuration of the load balancing groups.)
- If you have configured upstream shared spectrum groups while doing downstream load balancing, the downstream in each MAC domain must not use overlapping upstream groups. For example, the downstream in one MAC domain could use an upstream spectrum band of 10 to 30 MHz, while the

downstream in a second MAC domain could use an upstream spectrum band of 30 to 42 MHz. Each MAC domain has its own upstream shared spectrum group, allowing the load balancing group to contain the downstreams for both MAC domains.

Note A MAC domain is one downstream and its associated upstreams.

- All upstream ports coming from the same splitter must be using different center frequencies that are separated by the channel width. For example, if the upstreams are using a channel width of 3.2 MHz, the center frequencies for all upstreams must be separated by at least 3.2 MHz.
- You can use four initialization techniques for Dynamic Channel Change (DCC).
- As required by cable interface bundling, all interfaces in a load balancing group must also be in the same Hot Standby Connection-to-Connection Protocol (HCCP) interface bundle.
- If you have configured load balancing, the provisioning system must not assign specific upstream channels or downstream frequencies to individual cable modems in their DOCSIS configuration files. Any cable modems requiring specific upstream channels or downstream frequencies must be excluded from load balancing operations (using the **cable load-balance exclude** command).
- Do not use the utilization method of load balancing on cable interfaces that have a small number of cable modems and where a single modem is responsible for the majority of the interface load. In this condition, the Cisco CMTS could end up continually moving cable modems from one interface to another in an endless attempt to load balance the interfaces. To avoid this, configure the utilization threshold to a value that is higher than what can be caused by any single cable modem.
- You should not configure an interface for both dynamic load balancing and Hot-Standby Connection-to-Connection (HCCP) N+1 redundancy, because cable modems will go offline after a switchover. You can configure the interface for HCCP N+1 redundancy when you are using only static and passive load balancing.
- Load balancing, however, does not continue after a switchover from a Working to a Protect interface. Load balancing resumes when the Cisco CMTS switches back to the Working interface. (One possible workaround is to preconfigure the Protect interface with the appropriate load balancing commands, but you must be certain that the downstreams and upstreams in each load balancing group after the switchover have the same physical connectivity.)
- When deployed with channel restriction features, if the target upstream channel attribute masks are against that of the cable modem, then the cable modem on the higher load upstream will not be load balanced, as the current load balancing moves cable modems only to the target upstream. However, cable modems that do not have an attribute mask can still be load balanced. You should consider the following while deploying the load balancing groups: the target upstream will always be the upstream that has the lowest load. If some other upstreams have the same load, the upstream with the lowest index will be chosen as the target upstream.
- A TLV in a cable modem configuration file restricts dynamic load balancing on per modem basis. Still, existing static load balancing using frequency override technique and passive load balancing takes action at ranging time.
- If you remove the last rule of a DOCSIS policy, the policy itself will be removed.
- The Cisco CMTS load balancing feature moves a cable modem based on the load of the channels in a load balancing group, without checking if the cable modem supports the extended frequency range (5Mhz-85Mhz). This may result in moving a cable modem that supports standard frequency range

(5Mhz-65Mhz) to a channel that has extended frequency configured. To overcome such scenarios, operators should not mix upstreams that have standard and extended frequencies configured into the same load balancing group, unless all modems in the group support extended frequency range.

Restrictions for Dynamic Channel Change for Load Balancing

- DCC initialization 0 is the default technique for load balancing DCC.
- DCC initialization techniques 1-4 are strictly for downstream channel changes within a distributed line card (intra-card), and can not be used for load balancing between cards (inter-card). For load balancing between cards (inter-card), DCC initialization technique 0 will be used in all cases, regardless of what technique is set for the LB group or what card types are used.
- For load balancing between cards (inter-card), DCC initialization technique 0 will be used in all cases, regardless of what technique is set for the LB group or what card types are used.
- For load balancing between multiple cable interface line cards (inter-card implementation), DCC initialization technique 0 is to be used in all cases, regardless of what technique is set for the load balancing group or which cable interface line card types are used.
- The source and target upstreams and downstreams must share physical connectivity with the modem desired for a DCC transaction.
- Independent downstream change is not supported, and cross-MAC domain upstream changes must occur with the associated downstream changes.
- The source and target downstream interfaces must belong to the same virtual bundle and the same load balancing group if DCC is used for load balancing.
- For DCC initialization techniques 1 to 4, all the configuration variables of the cable modem must remain constant with the exception of the configuration variables that are explicitly changed by the Dynamic Channel Change request (DCC-REQ) messages encoding.
- DCC initialization techniques 2 to 4 must not be used if the propagation delay differences between the old and new channels exceeds the ranging accuracy requirement defined in DOCSIS, for example, ±0.25 usec plus ± symbol time.

  For example, for a symbol rate of 1.28 Msps, the timing offset difference between the source and target upstream channel is ± floor[(0.250 us + 0.5*0.781us)/(1/10.24)] = ± 6.
- The attenuation or frequency response differences between the old and new upstream channels causes the received power at the Cisco CMTS to change by more than 6 dB.
- DCC initialization technique 3 must not be used if the conditions for using technique 2 are not met.
- DCC initialization technique 4 must not be used if the conditions for using technique 2 cannot be met.
- Micro-reflections on the new upstream channel result in an unacceptable BER (greater than 1e-8) with pre-equalization coefficients set to the initial setting.
- DCC is used only for dynamic downstream load balancing on DOCSIS 1.1 and later CMs. Upstream Channel Change (UCC) is always used for dynamic upstream load balancing on DOCSIS 1.x CMs. For DOCSIS 2.x CMs, UCC is used when the *ucc* option is configured. For DOCSIS 3.x CMs, DCC is used irrespective of whether the *ucc* option is configured or not.
- Prolonged interruption of the multicast traffic is expected if the cable modem moved by DCC is the first one in a dynamic multicast group on the target interface. The downstream multicast service flow cannot

be reestablished until the Cisco CMTS receives an Internet Group Management Protocol (IGMP) join message from the customer premises equipment (CPE) as the result of the Cisco CMTS IGMP query, where the IGMP query interval is set to one minute. This is an IGMPv2 limitation.

- Effective with Cisco IOS Release 12.2(33)SCB5, multiple statically-assigned IP addresses to a CPE can be pinged. However, this works only if all the security features, such as verification of IP addresses for cable modems and CPE devices on the upstream, and other security mechanism are disabled.
- Multiple statically-assigned IP addresses to a CPE can be pinged. However, this works only if all the security features, such as verification of IP addresses for cable modems and CPE devices on the upstream, and other security mechanism are disabled.
- The TCS and RCS assigned to the DOCSIS 3.0 cable modems are restricted by the upstream and downstream bonding groups configured by the Cisco CMTS.
- Load balancing and DCC are not supported for CMs that are enabled for Layer 2 VPN (L2VPN) support.
- When a DCC occurs, the cable modem US and DS counters are reset. The US and DS counters include counters such as data and throughput seen in the **show cable modem** (**mac-address**) **verbose** command output and packets and bytes seen in the **show cable modem (mac-address) counters** command output.

DCC Restrictions with N+1 Redundancy and Inter-Card Load Balancing

- Inter-card load balancing is not supported with cable interface line cards using N+1 redundancy. Refer to general DCC restrictions for additional information.
- Dynamic load balancing should not be used together with N+1 redundancy. Cable modems with outstanding DCC transactions go offline after a switchover event.

Note When cable modems go offline during a switchover event, the load balancing feature activates. Cable modems move in relation to the switchover event. When the cable modems return online, load balancing may need to initiate again.

To facilitate load balancing during a switchover, you can increase the dynamic load balance threshold, if a certain percentage of cable modems that reset during switchover is configured in the system. An alternate method is to use static load balancing with N+1 redundancy. For more information, see the Types of Load Balancing Operations.

Restrictions for DOCSIS 3.0 Static Modem Count-Based Load Balancing

- Effective with Cisco IOS Release 12.2(33)SCF, static modem count-based load balancing is supported on MTC and MRC-only cable modems. Single-channel, narrowband cable modems will continue to be supported with dynamic load balancing as in the Cisco IOS Release 12.2(33)SCE and earlier releases. MRC-only modems are supported by dynamic load balancing on upstream channels.

Note DOCSIS 3.0 static modem count-based load balancing is not supported on:

- Multiple line cards.
- Load balancing groups and downstream channels shared across multiple line cards. However, autonomous load balancing-based CM steering and load balancing group assignment is supported across multiple line cards.

- In Cisco IOS Release 12.2(33)SCF, DOCSIS 3.0 static modem count-based load balancing does not support service flow method of load balancing.

Restrictions for Dynamic Bonding Change for DOCSIS 3.0 Static Modem Count-Based Load Balancing

- The Cisco CMTS can use only DBC messaging to move modems within a MAC domain and applies only to cable modems operating in MTC mode or MRC-only mode without a primary downstream change.
- The Cisco CMTS moves the MRC-only cable modems with a primary channel change using DCC with initialization technique 0.
- The Cisco CMTS moves cable modems across MAC domains using only DCC with initialization technique 0.
- The Cisco CMTS must ensure minimum interruption to existing QoS services while considering an initialization technique that is suitable for the cable plant conditions.
  - Initialization Technique 0—(Reinitializing the MAC) results in the longest interruption of service. This technique is used when QoS resources are not reserved on the new channel(s), when the downstream channel of an MRC CM is changed, or when the upstream channel of a CM to which a transmit channel change (TCC) was assigned in the registration process, is changed.

    Note Initialization technique 0 is used only with DCC, and not with DBC.

  - Initialization Technique 1—(Broadcast initial ranging) may result in a lengthy interruption of service, which is mitigated by the reservation of QoS resources on the new channel(s). The service interruption can be further reduced if the Cisco CMTS supplies the UCD TLV in the DBC request in addition to providing more frequent initial ranging opportunities on the new channel.
  - Initialization Technique 2—(Unicast ranging) offers the possibility of only a slight interruption of service. To use this technique, the Cisco CMTS must include the UCD TLV in the DBC message if the upstream channel is changing.
  - Initialization Technique 3—(Broadcast or unicast ranging) offers the possibility of only a slight interruption of service. Use this technique when there is uncertainty when the CM may execute the DBC command and thus a chance that it might miss station maintenance slots. However, the Cisco CMTS should not use this technique if the conditions for using techniques 1 and 2 are not completely satisfied.

- Initialization Technique 4—(Use the new channel directly) results in the least interruption of service.

- For a DOCSIS 3.0 cable modem that in a DOCSIS 3.0 static load balancing group, the multicast join will be dropped before REG-HOLD time elapses.

Restrictions for MRC-Only Cable Modems

- MRC-only cable modems use single channel non-bonded upstreams (similar to narrowband (NB) modems) and multi-channel bonding groups on the downstream.

Note The following restrictions apply only to DOCSIS 2.0 and DOCSIS 3.0 cable modems in MRC-only mode.

- cable modems are moved across upstream channels using DCC.
- cable modems are moved across downstream channels using DBC, if there is no change in the primary downstream channel; otherwise DCC with init tech 0 is used.
- cable modems are moved to different downstream channels through DBC, if there is a change in the upstream channel and downstream channel bonding group, but not in the primary downstream channel and the upstream channel change is ignored.

  However, if there is a change in the primary downstream channel also, DCC with init tech 0 is used to balance the cable modems.
- MRC-only modems are treated similar to cable modems operating in MTC mode, to move modems across downstream channels. For change in upstream channel, MRC-only cable modems are treated similar to single-channel NB cable modems.

Information on the Load Balancing on the Cisco CMTS

This section describes the operation, concepts, and benefits of the Load Balancing on the Cisco CMTS feature:

Feature Overview

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 re-balance 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.

This feature has been enhanced to make use of DOCSIS policies and rules to limit the movement of cable modems within a Load Balancing Group. A policy defines whether and when cable modems can be moved within their load balancing groups.

A policy consists of a set of rules. Each rule can be defined as “enabled”, “disabled”, or “disabled during time period.” Multiple policies can share a single rule. However, if you remove the last rule of a policy, that will also remove the policy.

Each rule can be used in any number of policies. When it is defined by multiple rules, all rules apply in combinations. Each rule helps to prohibit load balancing using a particular cable modem and to prohibit load balancing using a particular cable modem during certain times of the day.

Following are the general guidelines for the rules and policies:

- The policy or rule is recognized by a 32-bit ID.
- Each cable modem can have one policy only.
- Each rule can be associated to one or more policies.
- Each policy is described by at least one rule, otherwise it cannot be created.
- The zero Policy ID is reserved by Cisco CMTS indicating “Do nothing to LB prohibition.”
- If the policy ID specified by the cable modem configuration file is not configured on Cisco CMTS, no LB prohibition is applied to that CM. However, after the policy with the matched ID is configured, LB prohibition takes effect immediately.

DOCSIS 3.0 Static Modem Count-Based Load Balancing

Effective with Cisco IOS Release 12.2(33)SCF1, DOCSIS 3.0 static modem count-based load balancing supports the following:

The static modem count-based load balancing supports the following:

- DOCSIS General and Restricted load balancing group assignment to include DOCSIS 3.0 cable modems in MTC and MRC-only modes.

Note DOCSIS 3.0 static modem count-based load balancing is not supported:

  - Across multiple line cards.
  - For load balancing groups and downstream channels shared across multiple line cards. However, autonomous load balancing-based CM steering and load balancing group assignment is supported across multiple line cards

- Use of DCC and DBC in load balancing.
- Use of DBC for MRC-only modems during downstream move.
- Use of DCC with init tech 0 if the primary downstream channel is changed for MRC-only CMs.
- Use of DBC for cable modems in MTC mode for all upstream and downstream modem move.

- Separate counters for NB and wideband (WB)/upstream bonding (UB) CMs. For more information, see the **show cable load-balance docsis-group** command in the Cisco IOS CMTS Cable Command Reference.
- Aggregate logical channels to physical channels for load balancing. Physical channel load is calculated by using average weights among all logical channels.
- Non-primary downstream channels load where utilization of SPA QAM is considered

Note Dynamic DOCSIS load balancing is not supported in Cisco IOS Release 12.2(33)SCF.

Note DOCSIS 3.0 static modem count-based load balancing is the only LB method for wideband modems. When the CM counts across different WB interfaces are within predefined threshold levels, the load is always considered as balanced; no more CM move is initiated by the LB system. No service flow count, whether primary or secondary, is taken into consideration during this LB process.

Note When the CM counts across different WB interfaces are within predefined threshold levels, the load is always considered as balanced; no more CM move is initiated by the LB system. No service flow count, whether primary or secondary, is taken into consideration during this LB process.

Note The attributes considered for the forward interface for the service flow (SF) are attribute mask and available bandwidth, and *not* the number of service flows on each channel. If a channel is within the new RCS, then irrespective of the type of narrowband SF, (whether primary or secondary, or static or dynamic) the SF continues to use its current channel.

Note The US Phy Mode counters (scdma, atdma, and tdma) remain 0 for the UB interfaces.

DOCSIS 3.0 static modem count-based load balancing is based on legacy load balancing and supports any type of channel combination (upstream and downstream)—MxN, with 1x1 combination being the subset.

DOCSIS 3.0 static modem count-based load balancing controls dynamic changes to the set of downstream and upstream channels used by a registered CM. It supports the following:

- Multiple channel load balancing operation.
- Load balancing operation based on policies and priorities.
- Load balancing with multicast. DOCSIS 3.0 static modem count-based load balancing does not move any CM with active video sessions.

DOCSIS 3.0 static modem count-based load balancing supports the modem count-based load balancing in a hybrid deployment of DOCSIS 1.x, 2.0 and 3.0 cable modems.

Static modem count-based load balancing is supported only for DOCSIS 3.0 CMs. Single-channel, narrowband cable modems will continue to be supported with dynamic load balancing as in the Cisco IOS Release

12.2(33)SCE and earlier releases. MRC-only cable modems are supported by dynamic load balancing on upstream channels.

Error Handling of Channel Assignment

In Cisco IOS Release 12.2(33)SCE and earlier releases, the interface state of the channels is considered when determining LBG assignment. Only those channels that are in the "initial", "up", "suspicious", or "testing" states are available for LBG assignment.

However, in Cisco IOS Release 12.2(33)SCF, this restriction is modified. As long as the interface state of the channels is not "administratively down", all channels are available for LBG assignment. For other load balancing operations, such as moving modems using DCC, UCC, or DBC, the interface state of the channels should be in "initial", "up", "suspicious", or "testing" states.

As long as the interface state of the channels is not "administratively down", all channels are available for LBG assignment. For other load balancing operations, such as moving modems using DCC, or UCC, the interface state of the channels should be in "initial", "up", "suspicious", or "testing" states.

Multiple Channel Load Balancing Operation

CMs load balance in MRC and MTC modes. The following rules apply while load balancing CMs operating in these modes:

- For CMs operating in MRC and MTC modes, DBC is used to move CMs across downstreams by changing the RCS of the CM within same MAC domain.

  CMs operating in MRC-only mode can be moved across upstreams only through a DCC request. However, the Cisco CMTS uses DCC with initialization technique 0 (reinitializing the MAC domain) when changing the downstream channel of a CM operating in MRC mode.

- During CM registration, the Cisco CMTS may send a multipart registration response (REG-RSP-MP) message to include a TCC TLV encoding to the CM. This CM is marked as TCC-capable.

  For CMs operating in MRC, non-MTC, non-TCC-capable mode, load balancing uses:

  - DBC to change RCS of the CM
  - DCC to change upstream channel of the CM

- For CMs operating in narrowband mode, DCC is used to move CMs within and across MAC domains.

The tables below provide a snapshot view of the load balancing methods and the operations used to move bonded and non-bonded CMs in Cisco IOS Release 12.2(33)SCF1.

Table 39: Load Balancing Method to Move Bonded and Non-bonded CMs

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Dynamic Service Charge (Initialization Technique)	
				Within MAC Domain	**Across MAC Domains**

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Dynamic Service Charge (Initialization Technique)	
DOCSIS 3.0 CM in MTC mode	DOCSIS 3.0 static modem count-based load balancing (MCBLB) DOCSIS 3.0 dynamic load balancing	WB/UB	DS/US	DBC **Note** When DOCSIS 3.0 LB is enabled, and the MTC CM is outside RLBG, CM is moved inside RLBG.	DCC init tech 0
DOCSIS 3.0/D2.x CMs in MRC-only mode	DOCSIS 3.0 static MCBLB DOCSIS 3.0 dynamic load balancing	WB/UB	No change to the primary DS channel	DBC **Note** When DOCSIS 3.0 LB is enabled and CM with all DSs is outside RLBG, CM is moved inside RLBG.	DCC init tech 0
			Change to the primary DS channel	DCC init tech 0 **Note** CM with primary DS outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC init tech 0
DOCSIS 3.0 CMs in MRC-only mode	DOCSIS 2.0 static and dynamic MCBLB, dynamic utilization	NB	US	DCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC init tech 0
D2.x CMs in MRC-only mode	DOCSIS 2.0 static and dynamic MCBLB, dynamic utilization	NB	US	DCC/UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC init tech 0
DOCSIS 2.0 /DOCSIS 1.1 CMs in NB mode	DOCSIS 2.0 dynamic MCBLB, dynamic utilization	NB	DS	DCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC init tech 0
			US	UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	UCC

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Dynamic Service Charge (Initialization Technique)	
DOCSIS 1.0 in NB mode	DOCSIS 2.0 dynamic MCBLB, dynamic utilization	NB	DS	Force reinitialize CM **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	Force reinitialize CM
			US	UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	UCC

Table 40: Using DCC/DBC to Load Balance Bonded and Non-bonded Cable Modems

Channel	CM in MRC, MTC Mode	CM in MRC, non-MTC Mode	DOCSIS 1.1/2.0 CMs with Single US/DS	DOCSIS 1.0 CMs with Single US/DS
Upstream (US)	DBC	DCC	DCC	UCC
Downstream (DS)	DBC (within the same MAC domain)	DBC (within the same MAC domain)	DCC (within the same MAC domain)	Force reinitialize CM
	DCC with initialization technique 0 when moving CMs across MAC domains	DCC with initialization technique 0 when moving CMs across MAC domains	DCC with initialization technique 0 when moving CMs across MAC domains	Force reinitialize CM

Using DBC for DOCSIS 3.0 Load Balancing Movement

Effective with Cisco IOS Release 12.2(33)SCF1 and as part of the DOCSIS 3.0 specifications, at any time after registration, the Cisco CMTS uses the DBC command to change any of the following parameters in a DOCSIS 3.0 CM:

- Receive channel set
- Transmit channel set
- DSID(s) or DSID associated attributes
- Security association(s) for encrypting downstream traffic
- Service Flow Cluster Assignments

Note In Cisco IOS Release 12.2(33)SCF, only RCS and TCS are used by the DOCSIS 3.0 static modem count-based load balancing.

Use the **show cable load-balance docsis-group** command to display the current, real-time statistics for load balancing operations. For more information, see the Cisco CMTS Cable Command Reference.

Using DBC to Change the Receive Channel Set

The Cisco CMTS can add, delete, or change the channels in the RCS of a cable modem by including a RCC in the DBC-REQ.

If an RCS change affects the primary downstream channel of the cable modem, the cable modem is required to re-register on its upstream channels.

If channels are deleted from the RCS, the Cisco CMTS may stop sending traffic on the downstream channel to be removed, which may cause loss of traffic. The Cisco CMTS minimizes packet loss by duplicating traffic on the new and old RCS until it receives a DBC-RSP from the cable modem.

If the Cisco CMTS does not receive the DBC-RSP after six retries of the DBC-REQ, and the RCC change affects the primary downstream channel of the cable modem, the Cisco CMTS reinitializes the cable modem. If the RCC change does not affect the primary downstream channel of the cable modem, the RCS of the cable modem must be synchronized between the cable modem and the CMTS.

If the Cisco CMTS does not receive the DBC-RSP after six retries of the DBC-REQ, the Cisco CMTS reinitializes the cable modem.

Note For cable modems in MRC-only mode, a downstream channel move is initiated by a DBC message. However, DCC initialization technique 0 is used if there is a change in the primary downstream channel.

Using DBC to Change the Transmit Channel Set

The Cisco CMTS can add, delete, or replace one or multiple channels in the TCS in a single DBC message. Whenever the TCS of the cable modem changes, the CMTS appropriately modifies the service identifiers (SIDs) associated with the affected service flows.

A change in the TCS is accompanied by a valid initialization technique.

Using DBC to Change the Downstream ID

Using DBC, the Cisco CMTS can change the following attributes of a downstream ID (DSID):

- Re-sequencing encodings:
  - Downstream re-sequencing channel list—The CMTS can add, delete, and replace channels in the DS re-sequencing channel list.
  - DSID re-sequencing wait time—The CMTS can indicate a change in skew due to network or configuration changes through DSID re-sequencing wait time.
- re-sequencing Warning Threshold
- CM-STATUS Hold-Off Timer for Out-of-range Events
- Multicast Encoding—The CMTS can initiate a DBC transaction to either add, deleted, or change attributes of an existing multicast DSID:

- Client MAC Address
- Multicast cable modem interface Mask
- Group MAC Address

Using DBC to Change the Security Association for Encrypting Downstream Traffic

- The CMTS can initiate a DBC transaction to add or delete Security Associations (SA) used to encrypt downstream traffic.
- The CMTS cannot send a DBC request to a cable modem that is not in the "Authorized" State.
- The CMTS can send a DBC request with an SA that uses a cryptographic suite unsupported by the cable modem. However, if the cable modem receives a DBC request with an SA that it is not capable of using, the cable modem rejects the DBC request.

Using DBC to Change the Service Flow SID Cluster Assignments

The Cisco CMTS uses the Service Flow SID Cluster Assignments TLV in the DBC request to assign new channels to a service flow, remove channels from a service flow, or replace one channel with another for a service flow.

Note Multiple actions can occur within a single DBC message.

Types of Load Balancing Operations

The Load Balancing on the Cisco CMTS feature provides a more comprehensive load balancing solution by adding new forms of registration-based and dynamic load balancing. In Cisco IOS Release 12.2(15)BC1, the Load Balancing on the Cisco CMTS feature supports the following configurable types of load balancing:

- Static load balancing—This is a form of registration-based load balancing that is done at the time a cable modem registers. When a cable modem sends its registration request (REG-REQ) and ranging request (RNG-REQ) messages, the Cisco CMTS responds with a ranging response (RNG-RSP) message that includes either a Downstream Frequency Override or an Upstream Channel ID Override field that instructs the cable modem which channels it should use.
- Static load balancing—This is a form of registration-based load balancing that is done at the time a cable modem registers. The first phase of static load balancing is completed when the cable modem registers and path-selection occurs. The static load balancing operation is completed when the second phase occurs after the mandatory REG-HOLD time elapses after the cable modem is registered. .
- Passive load balancing—This is a form of registration-based load balancing that can be configured for individual cable modems. In this mode, the Cisco CMTS does not need to send any type of messaging to the modem. The Cisco CMTS ignores the RNG-REQ message from a cable modem that is attempting to register using a downstream or upstream that is currently overloaded. The cable modem repeats its registration request until it reaches a channel that can accept additional modems.

Note By default, the Cisco CMTS uses static load balancing, but passive load balancing can be specified for individual older cable modems (using the **cable load-balance exclude** command) that do not respond well to the static form. This method should be used only as needed because when used for a large number of modems, it could generate a large volume of ranging retry messages.

- Dynamic load balancing—This is a form of load balancing in which cable modems are moved among upstreams and downstreams after their initial registration and they come online, while potentially passing traffic. Cable modems that are currently online are moved when the load difference between two interfaces exceeds a user-defined percentage.

  Note The dynamic form of load balancing could be considered a form of traffic-based load balancing, in that cable modems could be moved between interfaces while they are passing traffic. However, the load balancing algorithms do not take into account the nature of traffic when considering which cable modems should be moved.

  When using dynamic load balancing and an upstream channel is overloaded, the Cisco CMTS sends an UCC request to a cable modem to instruct it to move to another upstream. The cable modem should move to the new upstream channel, without going offline or having to re-register with the Cisco CMTS.

  When using dynamic load balancing and a downstream channel is overloaded, the Cisco CMTS sends an abort response to a cable modem's ranging request (RNG-REQ) message. When the cable modem sends new REG-REQ and RNG-REQ messages, the Cisco CMTS specifies the new downstream channel in the Downstream Frequency Override field in its RNG-RSP message. The cable modem must go offline and re-register on the new downstream channel, so as to conform to the DOCSIS 1.0 specifications.

  During dynamic load balancing, the specified policy of the cable modem is checked to determine whether the cable modem is allowed to move. The load balancing policies are configured on the Cisco CMTS to limit the movement of CMs within a LBG. The cable modem will forward TLV43.1 in its REG-REQ message, which is then parsed and stored in the Cisco CMTS. A policy defines whether and when CMs can be moved within their load balancing groups.

  Note The dynamic load balancing method results in cable modems going offline and having to re-register whenever the modems are moved between downstreams. This is because the DOCSIS 1.0 specification requires cable modems to re-register whenever the downstream is changed using the Downstream Frequency Override message. Cable modems should not go offline when being moved between upstreams.

In all cases, the load balancing is done by moving cable modems from the interface with the higher load to an interface with a lower load. For dynamic load balancing, the Cisco CMTS determines which online cable modems should be moved in a round-robin fashion. For static and passive load balancing, the Cisco CMTS moves cable modems only when they register or re-register.

Methods to Determine When Interfaces Are Balanced

In addition to selecting how interfaces should be balanced (using the static, passive, or dynamic types of load balancing), you can also select one of the following methods that the Cisco CMTS should use to determine when interfaces are balanced:

- Modems Method—Uses the number of active cable modems on an interface.
- Utilization Method—Uses the current percentage of utilization of an interface.
- Service-Flows Method—Uses the number of active service flow IDs (SFIDs) on an interface.

See the following sections for more information about each method.

Modems Method

The modem method of load balancing uses the number of active cable modems on an interface to determine the current load. This is a form of distribution-based load balancing, in which the absolute numbers of modems are used to determine whether interfaces are load balanced.

This method does not take into account the amount of traffic flowing through the cable modems, but the system does take into account the relative bandwidth of the channels being used, so that channels with higher bandwidths are allocated higher numbers of cable modems. This means that when interfaces are using different channel widths or modulation profiles, the system can assign different numbers of cable modems to the interfaces to achieve a balanced load. For example:

- Channel widths— If two upstreams are being load balanced, and one upstream is configured with a channel width of 1.6 MHz and the other upstream is configured for a channel width of 3.2 MHz, the Cisco CMTS allocates twice as many cable modems to the second upstream because its channel width is twice as large as the first upstream channel width.
- Modulation profiles— If one downstream is configured for 64-QAM and the other downstream is configured for 256-QAM, the Cisco CMTS allocates a proportionately larger number of cable modems to the second downstream so as to achieve a balanced load.

When both the channel width and modulation profile are set differently on two interfaces, the system calculates a "weight" value to use as a guide to determine the relative bandwidths of the interfaces.

Tip In a system with balanced loads, the interfaces will contain the same number of cable modems only when the interfaces are configured with the same channel width and modulation parameters.

Algorithm for Bonded Channel Cable Modem Load Balancing

Effective with Cisco IOS Release 12.2(33)SCF, during registration of the cable modem, the modem count-based method uses the number of active cable modems on the allowed RCS to determine the current load on each channel. After the modem is assigned an RCS, the Cisco CMTS does not move the cable modem even when traffic conditions change.

When a cable modem sends a registration request, modem count-based method of load balancing ranks the allowed receive channel sets (RCS) based on their modem count and assigns the set with the lowest number of CMs, to the ranging cable modem.

Primary Channel Load Display for Target RCS

Starting with SCH, this feature enables the bonded modems to be moved at the time of registration such that the primary channels are distributed evenly among the primary-capable channels apart from the load being balanced on the target DS channels. Modem method ranks the RCS based on their primary loads and assigns the set with the lowest primary load to the ranging cable modem.

An optional keyword **primary-load** has been added to the **show cable load-balance docsis-group** command to display the primary load of an RCS. For more information, see the Cisco CMTS Command Reference.

Although the modem count-based method distributes the cable modems fairly as they register, the following conditions may cause a system imbalance:

- A channel or groups of channels fail because of a planned (administrative shutdown) or unplanned event.
- While some cable modems may continue to operate in partial mode, some may re-register because of the failure and are reassigned to the channels that are active.
- When the failed channels become operational again, the cable modems do not re-register and the system is unbalanced.

In this case, the modem count-based method sends an SNMP trap to alert the operator, and the operator can choose to manually intervene to re-balance the cable modems by resetting the MAC domain to force all cable modems to re-register.

Note For cable modems in MRC and MTC modes, the modem count based load balancing method considers the number of active modems and service flows on the primary channels in the RCS and TCS of the cable modem.

Note Because a wideband SPA channel can be used by different line cards and across multiple MAC domains, the accurate modem count per channel is calculated by aggregating the actual count from all line cards.

Utilization Method

Note Only narrowband cable modems and upstreams of MRC-only cable modems participate in the utilization method.

The utilization method uses an interface's current percentage of utilization to determine the current load. This method uses the amount of traffic being sent over an interface, in the form of the percentage of total bandwidth being used. The system takes into account the relative throughput and bandwidth (as determined by the modulation profiles and channel widths) of each interface when evaluating the load on those interfaces.

For example, if two upstreams are being load balanced using the utilization method, and the first upstream has twice the bandwidth of the second upstream, the two upstreams are considered balanced when they reach the same percentage of utilization. The first upstream is carrying more traffic than the second upstream because it has a larger capacity for traffic, but the percentage of utilization will be the same.

Note The average utilization figure is reset only when the upstream is shut down, allowing the load balancing operation to be more accurate.

When either DBS or the Fairness Across DOCSIS Interfaces is enabled, the channel load will vary, which may affect the load balancing result.

Configurable Minimum Threshold under Utilization Method

Note The utilization method does not move cable modems for load balancing until the utilization of at least one of the interfaces reaches 25 percent. This is done to avoid the unnecessary moving of cable modems due to temporary spikes in an interface's utilization rate. The minimum utilization threshold of 25 percent is fixed and cannot be configured.

Cisco IOS Release 12.2(33)SCH introduces an enhancement to enable configuration of the minimum utilization threshold under Utilization Method. The minimum utilization threshold may be configured in a range of 10 to 90 percent.As a result the cable modems will be moved only when the configured minimum utilization threshold is reached on an interface.

To configure the minimum threshold under the Utilization method, use the **cable load-balance method-utilization min-threshold** command in global configuration mode. For more information, refer to **cable load-balance method-utilization min-threshold** command reference.

Service-Flows Method

Note Effective with Cisco IOS Release 12.2(33)SCF, the Service-Flows Method is deprecated.

The Service Flows method of load balancing uses the number of active service flows on an interface to determine the current load. This is a form of distribution-based load balancing, where the absolute numbers of service flows are used to determine whether interfaces are load balanced.

This method does not take into account the amount of traffic flowing on each SFID, but the system does take into account the relative bandwidth of the channels being used, so that channels with higher bandwidths are allocated higher numbers of SFIDs. This means that when interfaces are using different channel widths or modulation profiles, the system can assign different numbers of SFIDs to the interfaces to achieve a balanced load. For example:

- Channel widths—If two upstreams are being load balanced, and one upstream is configured with a channel width of 1.6 MHz and the other upstream is configured for a channel width of 3.2 MHz, the Cisco CMTS allocates twice as many SFIDs to the second upstream because its channel width is twice as large as the first upstream channel width.
- Modulation profiles—If one downstream is configured for 64-QAM and the other downstream is configured for 256-QAM, the Cisco CMTS allocates a proportionately larger number of SFIDs to the second downstream so as to achieve a balanced load.

When both the channel width and modulation profile are set differently on two interfaces, the system calculates a “weight” value to use as a guide to determine the relative bandwidths of the interfaces.

Tip In a system with balanced loads, the interfaces will contain the same number of SFIDs only when the interfaces are configured with the same channel width and modulation parameters.

Using Both Static and Dynamic Load Balancing

Dynamic load balancing can be used together with static load balancing. The user-configured threshold for dynamic load balancing must be equal to or larger than the user-configured threshold for static load balancing.

With this configuration, when a load imbalance occurs, the system initially uses static load balancing, moving cable modems among interfaces when the modems register. If the load imbalance continues to grow and eventually passes the dynamic threshold, the system begins moving cable modems using dynamic load balancing. Then, when enough cable modems have been moved to push the imbalance below the dynamic threshold, the system reverts to static load balancing until the load imbalance falls below the static threshold value.

Load Balancing Parameters

The Load Balancing on the Cisco CMTS feature supports static, passive, and dynamic load balancing on both upstream and downstream channels. You can configure downstreams and upstreams to use the same load balancing parameters, or you can configure upstreams and downstreams separately.

You can determine which cable interfaces should participate in load balancing operations. You can also choose which of the following methods should be used to determine the current load on a cable interface, and therefore determine whether cable modems should be moved:

- Number of active cable modems
- Number of active service flows
- Channel bandwidth utilization

You can also specify the threshold values that the Cisco CMTS should use to determine how to assign new cable modems to upstreams and downstreams for both types of load balancing. You can also configure whether cable modems with active Voice-over-IP (VoIP) calls should be moved, and if so, what thresholds should be used. You can also exclude certain cable modems from one or all of the different forms of load balancing.

Load Balancing Groups

To enable the load balancing on the Cisco CMTS feature, you first must create and configure a load balancing group, which specifies how load balancing should be performed. You then must assign cable interfaces to the load balancing group, at which point the Cisco CMTS begins performing load balancing on those cable interfaces.

You can use separate load balancing groups for upstreams or downstreams, or you can use the same load balancing group for both upstreams and downstreams. However, all cable interfaces in a load balancing group must share the same physical RF connectivity.

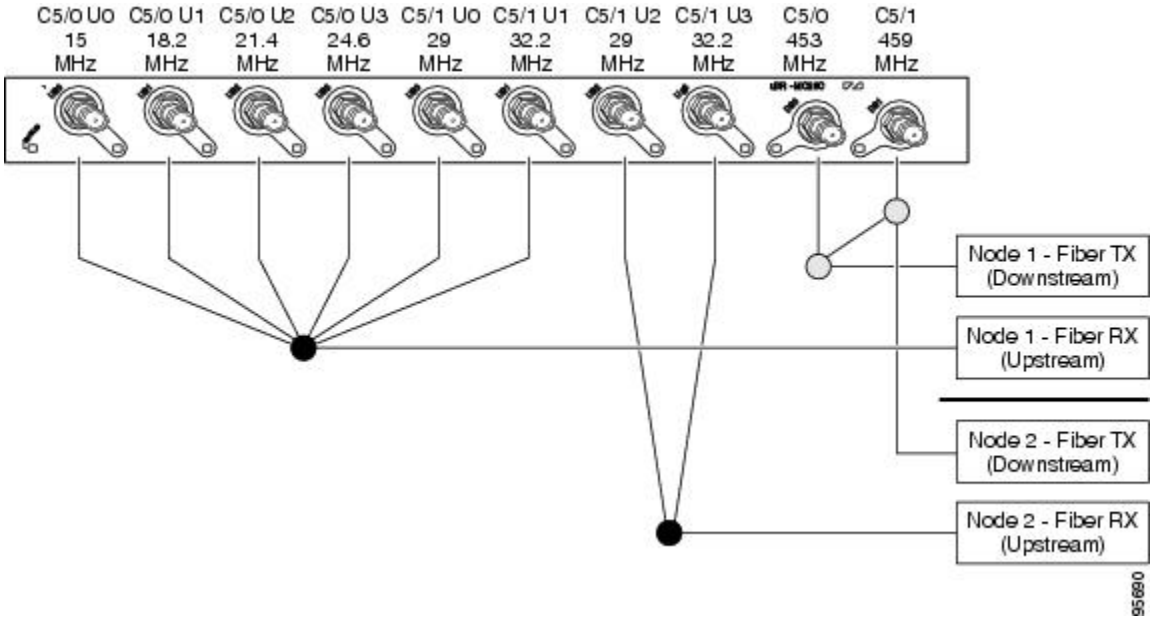
Note In later Cisco IOS releases, such as Cisco IOS Release 12.3(17a)BC, you can create a maximum of 80 load balancing groups on each chassis (the older limitation was 20). However, in prior Cisco IOS releases, you can reuse those load balancing groups on different sets of cable interfaces. If downstreams are not included in a load balancing group, then each downstream can be considered a separate domain.

Also, the same load balancing group must be used for all downstreams or upstreams that share RF connectivity and that are participating in load balancing. You cannot distribute downstreams or upstreams that share physical connectivity across multiple load balancing groups.

If you assign downstreams and upstreams to different load balancing groups, the Cisco CMTS performs load balancing independently on the upstreams and downstreams. If both downstreams and upstreams are assigned to the same load balancing group, the Cisco CMTS attempts to balance both the downstream and upstream load.

The figure below shows a simple example of how load balancing groups can be created.

Figure 6: Example of Load Balancing Groups



As shown in this figure, three load balancing groups are being used:

- All four upstreams for downstream C5/0 (U0-U3) and the first two upstreams (U0 and U1) for downstream C5/1 are used for the same node and are therefore part of the same load balancing group.
- The last two upstreams for downstream C5/1 (U2 and U3) are used for a different node and are therefore part of a separate load balancing group.
- The two downstreams, C5/0 and C5/1, are part of the same load balancing group, and this group is separate from the groups being used for the upstreams. (However, these downstreams could also be combined with one of the upstream load balancing groups.)

Note To see a sample configuration for this configuration, see the Example: Configuration for Upstreams and Downstreams, on page 452.

Support for 256 Legacy LBGs

To support effective configuration of legacy LBGs on the Cisco uBR-MC3GX60V line card, the valid range for the legacy load balance group is increased in Cisco IOS Release 12.2(33)SCE4. In Cisco IOS Release 12.2(33)SCE3 and earlier releases, the valid range was from 1 to 80. In Cisco IOS Release 12.2(33)SCE4 and later releases, the valid range is from 1 to 256.

Note Reuse of legacy LBGs across line cards of the same type is supported only on the Cisco uBR10-MC5X20, Cisco UBR-MC20X20V, Cisco uBR-MC28U, and Cisco uBR-MC88V line cards.

For an in-service downgrade, we recommend you remove the LBG configuration before the downgrade process, if legacy LBGs are configured with group IDs higher than 80. If you do not remove the configuration, these LBGs are automatically removed during the in-service downgrade process.

Downstream Load Balancing Distribution with Upstream Load Balancing

Downstream load balancing provides equalized load balancing with upstream group members. This enhancement synchronizes the "pending" statistic between different cable interface line cards in the load balancing group. The result is an alternative downstream load balancing scheme that makes use of per-upstream loads rather than total downstream loads.

This enhancement performs downstream load balancing that accounts for upstream channel loads 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 together.

The load balancing enhancement applies when downstream load balancing occurs on a headend system with separate upstream load balancing segments; the upstream segments are spread over multiple downstream segments.

The configuration and operation of making downstream load balancing decisions is enabled as follows:

- The target downstream segment is in the same downstream load balancing group as the source downstream segment.
- The upstream load balancing group can be set for the corresponding channel on which a cable modem is balanced.
- The Cisco CMTS automatically locates the upstream segment for a load balancing group and processes the upstream group status on the source interface that has the lowest load.
- The target downstream segment must have an upstream channel set in the upstream load balancing group.
- The highest target upstream segment must carry less load than any other potential target—the highest upstream segment on other interfaces.

For example, several upstream segments can be configured across multiple downstream segments as follows:

```
        U0      U1      U2      U3     Downstream
3/0     LB10    LB11    LB12    LB13      LB1
4/0     LB10    LB11    LB12    LB13      LB1
5/0     LB10    LB11    LB12    LB13      LB1
6/0     LB10    LB11    LB12    LB13      LB1
```

In this example, a cable modem that comes online on the interface cable 5/0 Upstream 2 could potentially come online on the following interfaces:

- cable 3/0 upstream 2
- cable 4/0 upstream 2
- cable 6/0 upstream 2

With downstream load balancing prior to Cisco IOS Release 12.3(17b)BC4, having 100 cable modems per segment would be possible in an extreme case that distributes cable modems as follows:

```
        U0      U1      U2      U3     Downstream
3/0     97       1       1       1        100
4/0      1      97       1       1        100
5/0      1       1      97       1        100
6/0      1       1       1      97        100
```

The enhancement enables the following advantages and behaviors:

- This enhancement adds support for synchronizing the "pending" statistic between different cable interface line cards and the network processing engine (NPE) so that a better decision can be made about where cable modems should be moved. This function can be used as a normal downstream load balancing implementation, if desired.
- This enhancement adds the **us-groups-across-ds** keyword to **cable load-balance group** command for configuring downstream load balancing groups with upstream resources.

Upstream Load Balancing for DOCSIS 3.0 Cable Modems in Single Upstream Mode

The upstream load balancing functionality enables the Cisco CMTS router to effectively handle upstream traffic for wideband and narrowband cable modems that are in single upstream mode. Single upstream mode (Mx1) means that the modems cannot send upstream traffic on multiple upstream channels. In the event of traffic overload on a single upstream channel of a wideband or narrowband cable modem, the Cisco CMTS router automatically moves the cable modem to another upstream channel in the same load balancing group.

Note A cable modem operating in single upstream mode is assigned to a load balancing group based on the primary channel of the modem. A cable modem in single upstream mode can support multiple receive channel (MRC) mode or narrowband mode. However, a cable modem in single upstream mode cannot support multiple transmit channel mode (MTC).

Disabling Upstream Load Balancing for DOCSIS 3.0 Modems

Effective with Cisco IOS Release 12.2(33) SCH1 and Cisco IOS Release 12.2(33)SCG6, you can activate load balancing only on downstream channels. This ensures that upstream load balancing is not activated,

allowing a maximum number of channels to be used to bring the upstream bonding cable modems online. This also prevents the CMTS from dynamically generating TCS different from the default single channel USBG, and user configured USBGs. For more information see Section *DOCSIS 3.0 Load Balancing with USBG Smaller than Cable Modem Capabilities* in the Upstream Channel Bonding

The Disabling Upstream Load Balancing for DOCSIS 3.0 Modems feature can be configured using the **downstream-only** keyword of the **cable load-balance docsis30-enable** command.

Disabling Upstream Load Balancing for DOCSIS 3.0 Modems

Effective with Cisco IOS Release 12.2(33) SCH1 and Cisco IOS Release 12.2(33)SCG6, you can activate load balancing only on downstream channels. This ensures that upstream load balancing is not activated, allowing a maximum number of channels to be used to bring the upstream bonding cable modems online. This also prevents the CMTS from dynamically generating TCS different from the default single channel USBG, and user configured USBGs. For more information see Section *DOCSIS 3.0 Load Balancing with USBG Smaller than Cable Modem Capabilities* in the Upstream Channel Bonding

The Disabling Upstream Load Balancing for DOCSIS 3.0 Modems feature can be configured using the **downstream-only** keyword of the **cable load-balance docsis30-enable** command.

DOCSIS 3.0 Dynamic Load Balancing

Effective with Cisco IOS Release 12.2(33) SCI, you can activate the DOCSIS 3.0 dynamic load balancing on the downstream channels. The DOCSIS 3.0 dynamic load balancing is based on the utilization method. It is used to balance the traffic across the QAM channels per load balance interval.

The DOCSIS 3.0 Dynamic Load Balancing feature can be configured using the **cable load-balance docsis30-dynamic-enable** command.

Note The DOCSIS 2.0 and DOCSIS 3.0 load balancing has to be enabled before configuring the DOCSIS 3.0 dynamic load balancing on Cisco CMTS.

Interaction with Spectrum Management

Cisco cable interface line cards support a number of features to maximize channel bandwidth and to minimize the impact of ingress noise on cable modem traffic. These features have the following impacts upon load balancing operations:

- Frequency hopping—Frequency hopping does not affect the load balancing algorithm, because it does not change either the bandwidth of a channel nor the number of cable modems on an interface.
- Dynamic modulation changes—The dynamic modulation feature affects the load balancing algorithm because it typically switches an interface from a higher-bandwidth modulation profile to a lower-bandwidth modulation profile in response to noise conditions on the interface.

  For example, if an upstream is configured for 16-QAM, sufficient noise levels could switch the upstream to a QPSK modulation profile. Depending on the load balancing configuration, this could then result in the movement of cable modems to other channels. Similarly, when the noise conditions improve, and the modulation is returned to the original, higher-bandwidth profile, the cable modems could be moved again to rebalance the upstream channels.

- Channel width changes—Multiple Cisco cable interface line cards, such as the Cisco uBR-MC16S/U/X, Cisco uBR-MC28U/X, and Cisco uBR10-MC5X20S/U/H, support automatic changes to the channel width in response to noise conditions. Because changing the channel width affects the throughput of a channel, this also affects the load balancing algorithm.

  For example, if noise makes the current channel width unusable, the Cisco cable interface line card reduces the channel width until it finds a usable channel width. Because this reduces the available bandwidth on the channel, the load balancing algorithm moves cable modems to rebalance the upstreams.

  In addition, the Cisco cable interface line card does not automatically restore the original channel width when noise conditions improve. Instead, the card changes the channel width only when it performs a subsequent frequency hop, either in response to additional noise conditions or when an operator performs a manual frequency hop. When the hop occurs, the card then searches for the largest possible channel width, and this could result in another movement of cable modems to rebalance the channels.

DOCSIS 2.0 Multicast Enhancement for VDOC

This feature enables the customer to tune a DOCSIS 2.0 cable modem to a specific downstream and supports static multicast video forwarding on it. The **vdoc-enabled** keyword enables the video over DOCSIS (VDOC) load balancing for static multicast groups.

The set-top boxes (STB) are configured with static video streams. The Cisco CMTS will check if the modems that are connected to these STBs are already on the specific downstream interface with these multicast replications when it receives joins for these static streams. If the modems are not on the correct downstreams, then a DCC message is sent to the line card to initiate the cable modem move to the correct downstream interface.

This feature is restricted by the following issues:

- Static multicast groups should be configured on the appropriate bundle interface as well as on the correct forwarding interfaces to enable this rule.
- This feature is not supported on load balancing groups which are derived from fiber node configuration and with multicast encryption.
- This feature does not support logical upstream channels.
- This feature works with DOCSIS 2.0 and 3.0 Multicast DSID-based Forwarding (MDF)-disabled cable modems.
- For MDF-enabled modems, the modem may support DCC but will not receive traffic till the next join arrives.
- It is highly recommended to have multicast QoS.
- The modems that support DCC due to load balancing will use init-tech 0 irrespective of the initialization technique configured on the load balancing group.
- This feature does not support multicast encryption. However, if the static group is configured for multicast encryption, then this feature will process the join and move the cable modem if required.

Benefits of Load Balancing

The Load Balancing feature on the Cisco CMTS provides the following benefits to cable service providers and their partners and customers:

- Provides a method that service providers can use for efficient bandwidth utilization, especially when using multiple upstream channels per fiber node.
- Allows service providers to expand their networks in an efficient manner, avoiding the cost of having to install additional fiber optic equipment and further segmenting the physical plant.
- Load balancing on downstream channels enables efficient bandwidth usage when using multiple downstream channels per fiber node to enable Video over IP and other services that require high-bandwidth real-time streams.
- Load balancing of upstream and downstream channels does not require any change to the provisioning servers or to any DOCSIS configuration files.
- Load balancing of upstream and downstream channels does not require any administrator or user intervention (such as manually resetting cable interfaces or manually rebooting cable modems).
- Load balancing can be used with the virtual interfaces feature, and with virtual interface bundling, on the Cisco uBR10-MC5X20S/U/H cable interface line cards, to provide load balancing for configurable MAC domains. Load balancing is also supported for virtual interface bundling with Cisco uBR-MC28U/X cable interface line cards.
- Allows service providers to equally balance their downstreams as cable modems register, so that cable modems do not all attempt to register on the same downstream, resulting in many cable modems failing to register and having to search for a new downstream.
- Cable modems can be moved among downstream and upstream channels without having to change any network parameters in manual fashion, such as IP address.
- Allows service providers to stay ahead of customers' bandwidth demands by dynamically responding to current load-usage conditions.
- Allows service providers to optimize the load balancing parameters for critical services, such as Voice over IP (VoIP).

Exclude Cable Modems from Load Balancing Groups

Load Balancing Process

The load balancing process has two phases.

- Assignment phase.

  When a modem is coming online in the assignment phase, the modem is moved to the load balance group by assigning it a load balancing group (LBG) ID. The assignment phase occurs only when a modem is coming online.

- Balancing phase.

  In the balancing phase, a modem is re-assigned to an LBG to balance the load.

Excluding Cable Modems from Load Balancing

Effective with Cisco IOS Release 12.2(33)SCH, there are four options that are used to exclude cable modems from an LBG:

- The **assignment** option:

The **assignment** option is used to exclude a modem during the assignment phase. The modem is not assigned an LBG and LBG ID is not displayed in the output of the **show cable modem verbose** command. The **assignment** option cannot be used when a modem is already online.

- The **static** option:

  The **static** option is used to exclude a modem during the Balancing phase. The modem is assigned to an LBG with an LBG ID. The **static** option is used to exclude a modem during static load balancing.

- The **enforce** option:

  The **enforce** option is similar to the **static** option, except that the **enforce** option is used to exclude a modem during dynamic load balancing.

When a cable modem is excluded from load balancing using the **assignment** option, the cable modem is not available for load balancing using the **static** or the **enforce** options.

- The **strict** option:

  The **strict** option excludes a modem in both the phases of load balancing. When a modem is online already, the **strict** option applies the **static** and the **enforce** options. It applies the **assignment** option only when the modem comes online again.

How to Configure Load Balancing

To configure load balancing groups, and to enable load balancing, refer to the configurations in the *DOCSIS Load Balancing Groups* document. Each task is marked as required or optional, as appropriate.

Creating a Load Balancing Group

This section describes how to create a load balancing group. You must create at least one load balancing group before the Cisco CMTS will begin load balancing cable modems.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance group** *n* **method** [**modems** | **service-flows** | **utilization**] **Example:** `Router(config)# cable load-balance group 10 method service-flows`	Creates a load balancing group.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating a Load Balancing Rule

This configuration is optional. You must create at least one load balancing rule before the Cisco CMTS can use load balancing policies.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance rule** *rule-id* {**disable-period** | **disabled** | **enabled** | **vdoc-enabled**} [**dis-start** *start-time* | **dis-period** *disable-period*] **Example:** `Router(config)# cable load-balance rule 1 disabled`	Creates a load balancing rule with the following parameters:
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Troubleshooting Tips

Problem When you disable load balancing and enable it for the next day using the **cable load-balance rule** *rule-id* **disable-period dis-start** *start-time* **dis-period** *disable-period* command, the load balancing is enabled at 12.00 am instead of the configured *disable-period*.

Possible Cause Load balancing rule cannot be disabled and enabled on the next day (that is, after 24 hours) using a single load balancing rule.

Solution Configure separate load balancing rules for disabling load balancing and enabling it on the next day. Configure the rule to disable load balancing using the **cable load-balance rule** *rule-id* **disable-period dis-start** *start-time* **dis-period 0** command. Configure the rule to enable load balancing using the **cable load-balance rule** *rule-id* **disable-period dis-start 0 dis-period** *disable-period* command to enable it for the next day.

Creating a Load Balancing Policy

This configuration is optional. You must create at least one load balancing rule before the Cisco CMTS can use a load balancing policy.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-policy** *policy-id* **rule** *rule-id* **Example:** `Router(config)# cable load-balance docsis-policy 2 rule 1`	Creates a load balancing rule with the following parameters: • *policy-id* —Specifies the DOCSIS policy to be created. • **rule** *rule-id*—Specifies the rule to be used with the DOCSIS policy.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring a Load Balancing Group

This section describes how to configure a load balancing group. All steps are optional, unless you want to change the default load balancing configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance group** *n* [**interval** *seconds*] **Example:** `Router(config)# cable load-balance group 10 interval 30`	Modifies the frequency by which the Cisco CMTS checks for exceeded thresholds in order to launch the load balancing feature. • *n* —Number of the load balancing group. In Cisco IOS Release 12.2(33)SCE3 and earlier, the valid range is from 1 to 80. In Cisco IOS Release 12.2(33)SCE4 and later, the valid range is from 1 to 256. • **interval** *seconds*—Minimum time interval taken for the CMs to move to load balance the interfaces. At least one CM is moved during each time interval. In Cisco IOS Release 12.2(33)SCE and earlier releases, the valid range is 1 to 1000 seconds, with a default value of 10. In Cisco IOS Release 12.2(33)SCE1 and later releases, the valid range is 1 to 1000 seconds, with a default value of 30.
Step 4	**cable load-balance group** *n* **threshold** {**load** *load-value* [**enforce** *threshold*] | **load minimum** *number* | **stability** *percent* | **ugs** *band-value*} **Example:** `Router(config)# cable load-balance group 10 threshold load 20 enforce 30`	Specifies the thresholds to be used to determine when cable modems should be moved to achieve the desired load balancing. • **load** *load-value*—Specifies the maximum load difference that can exist between interfaces in a group before the Cisco CMTS performs load balancing. The valid range for *load-value* is 1 to 100 percent, with a default of 10 percent. This value applies to static load balancing, used during cable modem registration. **Note** The default of 10 percent is the minimum recommended threshold. Do not set this threshold below 10 percent unless you have been instructed to do so by Cisco TAC. • **enforce** *threshold*—Enables dynamic load balancing, which moves online cable modems. The range for the *threshold* parameter starts from the current value of the *load-value* parameter up to 100 percent. The default equals the current value of the *load-value* parameter. • **load minimum** *number*—Specifies that cable modems should be moved only if the load between the two interfaces is greater than the specified number of cable modems or service flows (valid only when the method being used is the number of modems or service flows; it is not used for the utilization method). • **stability** *percent*—Specifies the minimum allowable percentage of good periodic ranging requests that is acceptable. When the channel has a lower

	Command or Action	Purpose
		percent of modems responding to the ranging requests in a one minute period, the Cisco CMTS begins moving modems. The valid range is 1 to 100 percent, with a default of 50 percent. • **ugs** *band-value*—Specifies that the Cisco CMTS should move cable modems with active Unsolicited Grant Service (UGS) service flows when the current UGS usage reaches the *band-value* percentage. The valid range for *band-value* is 0 to 100 percent, with a default of 70 percent.
Step 5	**cable load-balance group** *n* **policy** {**pcmm** | **ugs** | **us-groups-across-ds**} **Example:** `Router(config)# cable load-balance group 10 policy ugs` `Router(config)# cable load-balance group 10 policy pcmm` `Router(config)# cable load-balance group 10 policy us-groups-across-ds`	Allows the Cisco CMTS to move cable modems that have active UGS service flows to enforce the load balancing policy. • *n* —Number of the load balancing group. In Cisco IOS Release 12.2(33)SCE3 and earlier, the valid range is from 1 to 80. In Cisco IOS Release 12.2(33)SCE4 and later, the valid range is from 1 to 256.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Note The load balancing algorithms assume a relatively even distribution of usage among modems. In the situation where one cable modem creates the bulk of the load on an interface, the load balancing thresholds should be configured for a value above the load created by that single modem. You should check for this situation whenever the load balancing algorithm is moving a large number of modems from one interface to another.

Configuring the DOCSIS 3.0 Dynamic Load Balancing

This configuration is optional. This section describes how to enable the DOCSIS 3.0 dynamic load balancing on the downstream channels.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**cable load-balance docsis-enable** **Example:** `Router(config)# cable load-balance docsis-enable`	Enables DOCSIS 2.0 load balancing on the Cisco CMTS.
Step 4	**cable load-balance docsis30-enable** **Example:** `Router(config)# cable load-balance docsis30-enable`	Enables DOCSIS 3.0 load balancing on the Cisco CMTS.
Step 5	**cable load-balance docsis30-dynamic-enable** **Example:** `Router(config)# cable load-balance docsis30-dynamic-enable`	Enables DOCSIS 3.0 dynamic load balancing on the Cisco CMTS.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Assigning Interfaces to a Load Balancing Group

This section describes how to assign cable interfaces (both downstreams and upstreams) to a load balancing group. A cable interface does not participate in load balancing operations until it is a member of a load balancing group.

Restriction

- A downstream or upstream can belong to only one load balancing group.
- All downstreams and upstreams in a load balancing group must share physical connectivity to the same group of cable modems. Downstreams can be in a separate load balancing group than upstreams, but all downstreams or all upstreams that have the same RF physical connectivity must be members of the same load balancing group. You cannot distribute downstreams or upstreams that share physical connectivity across multiple load balancing groups.
- All interfaces in a load balancing group use the same load balancing parameters. By default, all cable modems on those interfaces are included in load balancing operations. However, you can exclude one or more particular cable modems from being moved in load balancing operations.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/port* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 4	**cable load-balance group** *n* **Example:** `Router(config-if)# cable load-balance group 10`	Assigns the downstream interface to the specified load balancing group.
Step 5	**cable downstream frequency** *freq-hz* **Example:** `Router(config-if)# cable downstream frequency 453000000`	Specifies the known downstream center frequency to be used on this cable interface. This is an information-only configuration on cable interfaces that use an external upconverter, but it is still required for load balancing so that the Cisco CMTS knows what frequencies it should use when moving cable modems from one downstream to another. The *freq-hz* parameter specifies the frequency in Hz, with a valid range of 54,000,000 to 858,000,000. Depending on the channel width, the range of center frequency that is acceptable to a CM is 91,000,000 to 857,000,000 Hz.
Step 6	**cable upstream** *uport* **load-balance group** *n*	Assigns an upstream port to the specified load balancing group.

	Command or Action	Purpose
	Example: `Router(config-if)# cable upstream 0 load-balance group 10`	**Note** Repeat Step 3, on page 439 through Step 6, on page 439 as needed for each downstream cable interface and its upstream ports that should belong to this group.
Step 7	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Excluding Cable Modems from a Load Balancing Group

This configuration is optional. This section describes how to exclude a particular cable modem, or all cable modems from a particular vendor, from participating in static or dynamic load balancing operations, and optionally marking the modems for passive load balancing. This task is optional, because, by default, cable modems on an interface participate in whatever load balancing operations have been configured.

Note This step might be required for some cable modems that are not DOCSIS-compliant. Such cable modems can go offline for long periods of time when load balancing is attempted using DOCSIS MAC messages. If this is the case, use the **cable load-balance exclude** command to exclude such cable modems from load balancing operations until the modem can be upgraded to DOCSIS-compliant software.

Tip You must exclude cable modems that require specific upstream channels or downstream frequencies. Load balancing cannot be done when cable modems are assigned specific channels or frequencies in their DOCSIS configuration files.

Support for Excluding Old Devices

Load balancing for old cable devices like Set Top Boxes (STBs) which do not support load balancing, will fail. In the output for **show cable load-balance group** command, these devices will show as 'suspicious' and then as 'disabled'. This will disrupt normal operations of other modems in the load balancing group. To exclude these STBs, a **cable load-balance exclude** command is configured to exclude each STB.

Note Starting with Cisco IOS Release 12.2(33)SCH, you can configure the **cable load-balance exclude** command once to exclude all the STBs, that do not support load balancing, instead of configuring the command several times with matched MAC addresses. You can also move cable modems that were moved to a load balancing group in assignment phase.

In Cisco IOS Release 12.2(33)SCH, the **cable load-balance exclude** modem command is modified to include the *mask* argument as an optional argument. The MAC address of a cable modem that belongs to the range specified by the MAC address mask, will be excluded by matching the "1" bit in mask. While configuring a new range rule using the *mask* argument, an existent rule with the same range is overwritten.

In Cisco IOS Release 12.2(33)SCH, the **cable load-balance exclude** modem command is modified to include the **assignment** option. This option allows you to exclude a cable modem that was moved into a load balancing group in assignment phase.

Note You can configure the **cable load-balance exclude** command once to exclude all the STBs, that do not support load balancing, instead of configuring the command several times with matched MAC addresses. You can also move cable modems that were moved to a load balancing group in assignment phase.

The **cable load-balance exclude** modem command is modified to include the *mask* argument as an optional argument. The MAC address of a cable modem that belongs to the range specified by the MAC address mask, will be excluded by matching the "1" bit in mask. While configuring a new range rule using the *mask* argument, an existent rule with the same range is overwritten.

The **cable load-balance exclude** modem command is modified to include the **assignment** option. This option allows you to exclude a cable modem that was moved into a load balancing group in assignment phase.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance exclude** {**modem** *mac-address* [*mac-mask*] | **oui** *oui-value*} [**assignment** | **enforce** | **static** | **strict**] **Example:** `Router(config)# cable load-balance exclude oui 00:00:0c`	Specifies that one or more cable modems should be excluded from load balancing operations. By default, the cable modems are excluded from dynamic and static load balancing, but they continue to participate in passive load balancing. Use the following options to exclude the cable modems from others combinations of load balancing:

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Disabling Load Balancing

This configuration is optional. Use the following commands to disable DOCSIS 3.0 static modem count-based load balancing:

```
Router(config)# cable load-balance docsis-group FN 1 MD cable 6/0/0
Router(config-lb-group)# disable
Router(config-lb-group)#
```

Legacy load balancing requires cable modems to re-register when load balancing configuration is changed.

With DOCSIS 3.0 static modem count-based load balancing, when load balancing related configuration within the LBG is changed as follows, the cable modems are forced to re-register:

- Partial shut or no shut interfaces under the LBG domain
- MRC or MTC mode in cable modems is turned on or turned off
- Change in fiber node for GLBG
- Change in wideband configuration for downstream group
- Change in the upstream bonding group

Use the following commands to force cable modems to re-register:

- **clear cable modem delete**
- **clear cable load state**
- **clear cable load counters**

Distributing Downstream Load Balancing with Upstream Load Balancing

Two commands are used to configure or display the configuration and status of distributed load balancing on the Cisco CMTS:

- **cable load-balance group** *ds-lb-group-id* **policy** {**pcmm** | **ugs** | **us-groups-across-ds**}
- **show cable load all**

The optional configuration of making downstream load balancing decisions is enabled as follows:

- The target downstream segment is in the same downstream load balancing group as the source downstream segment. This feature finds the target frequency and interface based on the upstream loads within the same upstream group as the source.

- The upstream load balancing group can be set for the corresponding channel on which a cable modem is balanced on the downstream channels.
- The Cisco CMTS automatically locates the upstream segment for a load balancing group and processes the upstream group status on the source interface that has the lowest load.
- The target downstream segment must have an upstream channel set in the upstream load balancing group.
- The highest target upstream segment must carry less load than any other potential target—the highest upstream segment on other interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance group** *ds-lb-group-id* **policy** {**pcmm** | **ugs** | **us-groups-across-ds**} **Example:** `Router(config)# cable load-balance group 1 policy us-groups-across-ds`	Sets the type of service flow policy for use with Load Balancing. This command synchronizes the pending statistic between different cable interface line cards in the load balancing group. The result is an alternative downstream load balancing scheme that makes use of per-upstream loads rather than total downstream loads when making load balancing decisions.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	**show cable load all** **Example:** `Router# show cable load all`	Displays load balancing statistics and status of load balancing configurations on the Cisco CMTS, to include distributed upstream-to-downstream load balancing when configured.

Examples

The following example illustrates this command and one supported implementation:

```
Router(config)# cable load-balance group 1 policy us-groups-across-ds
```

In this example, a cable modem that comes online on the interface cable 5/0 Upstream 2 could potentially come online on the following interfaces:

- cable 3/0 upstream 2

- cable 4/0 upstream 2
- cable 6/0 upstream 2

With downstream load balancing prior to Cisco IOS Release 12.3(17b)BC4, having 100 cable modems per segment would be possible in an extreme case that distributes cable modems as follows:

```
U0      U1      U2      U3     Downstream
3/0     97       1       1       1        100
4/0      1      97       1       1        100
5/0      1       1      97       1        100
6/0      1       1       1      97        100
```

The following example explores one collective configuration that follows the best practices and command syntax for this feature. In this example, additional configuration commands described elsewhere in this document configure Load Balancing as follows:

```
Router> enable
Router# configure terminal
Router(config)# cable load-balance group 6 method utilization
Router(config)# cable load-balance group 6 interval 60
Router(config)# cable load-balance group 6 threshold load 10 enforce
Router(config)# cable load-balance group 6 policy us-groups-across-ds
```

The following **show** command illustrates distributed downstream and upstream load balancing according to this feature in Cisco IOS Release 12.3(17b)BC4 and later releases:

```
Router# show cable load all

Group  Interval  Method      DCC Init     Threshold
                             Technique    Minimum  Static  Enforc gs   PCMM
1      10        modems      0             1        2%      2%      ---   ---
10     1         modems      0             1        1%      ---     ---   ---
11     1         modems      0             1        1%      ---     ---   ---

Current load:

Interface            State      Group Utilization  Reserved Modems Flows Weight
Cable5/0 (525 MHz)   up         1     0%(0%/0%)    0%       14     28    37
Cable5/0/U0          up         10    0%           0%       9      9     2.5
Cable5/0/U1          up         11    0%           0%       5      5     2.5
Cable6/0 (411 MHz)   up         1     0%(0%/0%)    0%       30     60    37
Cable6/0/U0          up         10    0%           0%       19     19    5.1
Cable6/0/U1          up         11    0%           0%       11     11    5.1

Target assignments:

Interface            State      Group  Target
Cable5/0 (525 MHz)   up         1
Cable5/0/U0          up         10
Cable5/0/U1          up         11
Cable6/0 (411 MHz)   up         1
Cable6/0/U0          up         10
Cable6/0/U1          up         11

Statistics:

Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable5/0 (525 MHz)     up         18        1         3         0
Cable5/0/U0            up         0         0         0         0
Cable5/0/U1            up         0         0         0         0
Cable6/0 (411 MHz)     up         12        0         6         0
Cable6/0/U0            up         0         0         0         0
Cable6/0/U1            up         0         0         0         0
```

How to Configure Dynamic Channel Change for Load Balancing

DCC and DCC for Load Balancing is supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router with the Cisco MC28U and the Cisco MC5X20S/U/H cable interface line cards.

DCC in DOCSIS 1.1 dynamically changes cable modem upstream or downstream channels without forcing a cable modem to go offline, and without reregistration after the change. DCC supports five different initialization methods (0-4), instead of one, as in earlier DOCSIS support.

Dynamic Channel Change (DCC) and DCC for Load Balancing on the Cisco CMTS supports the following:

- 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).
- Applications that are sensitive to delay, such as PacketCable (PC) and PacketCable MultiMedia (PCMM), may use DCC initialization technique 4 to retain services while the cable modem is performing DCC.
- If the channel is in mixed or ATDMA-only mode, the primary Service Identifier (SID) must be switched to ATDMA-only mode.

Configuring DCC for Load Balancing on the Cisco CMTS

To configure the DCC feature for load balancing, use the following steps. Values indicated are sample values that may differ from your own.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance group** *group-num* **dcc-init-technique** *number* **Example:** `Router(config)# cable load-balance group 1 dcc-init-technique 0`	Sets the DCC initialization technique for the specified load balancing group. The initialization technique number can range from 0 to 4.

	Command or Action	Purpose
Step 4	**cable load-balance group** *group-num* **policy** {**pcmm** | **ugs** | **us-groups-across-ds**} **Example:** `Router(config)# cable load-balance group 1 policy pcmm`	Enables load balancing of cable modems with PacketCable MultiMedia (PCMM) service flows, Unsolicited Grant Service (UGS) service flows, or both PCMM and UGS service flows. Applies these setting to the specified load balancing group.
Step 5	**cable load-balance group** *group-num* **threshold** {**load** | **pcmm** | **stability** | **ugs**} {*1-100*} **Example:** `Router(config)# cable load-balance group 1 threshold ugs 75`	Selects the type of service flow threshold and sets the respective threshold in a percentage for the load balancing group.
Step 6	**cable load-balance group** *group-num* **threshold load** {*1-100*} {**minimum**} **Example:** `Router(config)# cable load-balance group 1 threshold load 75 minimum`	Sets the load threshold for the specified load balancing group.
Step 7	**cable load-balance group** *group-num* **threshold load** {*1-100*} {**enforce**} **Example:** `Router(config)# cable load-balance group 1 threshold load 75 enforce`	Sets the enforce threshold for the specified load balancing group.
Step 8	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

To test and verify DCC for load balancing, use the following two commands:

- **test cable dcc**
- **show controllers cable**

These commands are described in the *Cisco CMTS Cable Command Reference* .

Verifying Load Balancing Operations

This section describes how to use certain test and show commands to verify the configuration and operation of the Load Balancing feature or Dynamic Channel Change feature on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**test cable load-balance** *mac-address* [**ucc** | **upstream**] [*count*] **Example:** `Router# test cable load-balance 0000.394e.4e59`	Tests the operation of the current load balancing configuration by moving a cable modem to a new upstream. **Note** You can create a maximum of 80 load balancing groups on each chassis.
Step 3	**show cable load-balance** [**group** *n*] [**all** | **load** | **pending** | **statistics** | **target**] **Example:** `Router# show cable load-balance group 1`	Displays real-time statistical and operational information for load balancing operations. If given without any options, this command displays information for the load balancing groups and each cable interface's current load and load balancing status. You can also specify the following options:
Step 4	**test cable dcc** [*mac-addr* | *ip-addr* | *cable-if-src sid*] *cable-if-target uschan* {*ranging-tech* } **Example:** `Router# test cable dcc 0000.394e.4e59`	Tests Dynamic Channel Change (DCC) by moving a target cable modem, as specified by MAC address, IP address, or the primary service ID (SID) value. Applies to a cable modem on the source interface to an upstream channel on a target downstream interface using the initialization technique specified.

Troubleshooting Tips

Problem Packets are dropped when a cable modem moves from one channel to another.

Possible Cause Effective with Cisco IOS Release 12.2(33)SCF, when the **test cable dcc** command is used to move a cable modem from one channel to another with DCC initialization technique 3:

- If the pre-equalization coefficient is enabled, the cable modem moves and packet drop occurs for 5 seconds.
- If the pre-equalization coefficient is disabled, the cable modem moves and packet drop occurs for less than 1 second.

Possible Cause Effective with Cisco IOS Release 12.2(33)SCF, when the **test cable dcc** command is used to move a cable modem from one channel to another with DCC initialization technique 4:

- If the pre-equalization coefficient is enabled, the cable modem moves and packet drop occurs for less than 1 second.
- If the pre-equalization coefficient is disabled, the cable modem moves without any packet drop.

Solution No action is required.

Examples

Use the **show cable load-balance target** command to display the interfaces being used for load balancing, use the **test cable load-balance** command to test whether a cable modem can move between interfaces, and use the **show cable load-balance statistics** command to display the results of the test.

The following example shows how to test whether a specific cable modem responds to both a UCC request and to an upstream channel override to move from one upstream to another in its load balancing group:

```
Router# show cable load-balance target

Target assignments:
Interface            State      Group  Target
Cable1/0/0 (669 MHz) up         1
Cable1/0/0/U0        up         1      Cable1/0/0/U1 [enforce]
Cable1/0/0/U1        up         1

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         33        0         1         0
Cable1/0/0/U1        up         22        0         2         0

Router# test cable load-balance 0000.394e.4e59

Sending UCC request: Cable1/0/0/U0 --> U1
Waiting for test completion ........
Test results:
    UCC Response: 0.0s
    Initial Ranging: 8.5s
    Ranging Complete: failed.
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 8.5s max 8.5s avg 8.5s
Testing US Channel Override: Cable1/0/0/U1 --> U0
Waiting for test completion ...........
Test results:
    Initial Ranging: 8.5s
    Ranging Complete: failed.
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 8.5s max 8.5s avg 8.5s

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         34        0         1         0
Cable1/0/0/U1        up         23        0         2         0
```

The following example shows how to test whether a specific modem responds to a UCC request to move from one upstream to another in its load balancing group:

```
Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         34        0         1         0
Cable1/0/0/U1        up         23        0         2         0
```

```
Router# test cable load-balance 0007.0e01.4129 ucc 1

Sending UCC request: Cable1/0/0/U0 --> U1
Waiting for test completion ........
Test results:
    UCC Response: 0.0s
    Initial Ranging: 10.3s
    Ranging Complete: 11.2s
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 10.3s max 10.3s avg 10.3s
    Ranging Complete: success rate 100% min 11.2s max 11.2s avg 11.2s

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         35        0         1         0
Cable1/0/0/U1        up         24        0         2         0
```

The following example shows information when moving a cable modem to a different upstream channel using DCC initialization technique 1. This example moves the cable modem 0012.17ea.f563 from interface c7/1/0 upstream 1 to interface c7/1/1 upstream 0 using DCC initialization technique 1:

```
Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (dB)   Offset  CPE Enb
 State       Sid  (dB)   Offset  CPE Enb
0012.17ea.f563 12.0.0.2        C7/1/0/U1 online      4    0.00  2449     0   N

Router# test cable dcc 0012.17ea.f563 c7/1/1 0 1

Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (dB)   Offset  CPE Enb
0012.17ea.f563 12.0.0.2        C7/1/1/U0 online      3    0.00  2451     0   N
```

Verifying Dynamic Bonding Change for Load Balancing

To verify the DBC parameters for load balancing, use the following commands:

- **show cable load-balance docsis-group**
- **show cable modem verbose**
- **show cable mac-domain cable** *slot/subslot/interface-index* **rcc**

The following is a sample output for the **show cable mac-domain cable rcc** command:

```
Router# show cable mac-domain cable 6/0/0 rcc 1

RCC ID                  : 1
RCP                     : 00 00 00 00 00
Created Via             : Wideband - Wi1/0/0:0
Receive Channels        : 4
  Receive Channel       : 1
    Center Frequency    : 423000000
    Primary Capability  : YES
  Receive Channel       : 2
    Center Frequency    : 429000000
    Primary Capability  : NO
  Receive Channel       : 3
```

```
    Center Frequency    : 435000000
    Primary Capability  : NO
  Receive Channel       : 4
    Center Frequency    : 441000000
    Primary Capability  : NO
Receive Modules         : 1
  Receive Module        : 1
    First Frequency     : 423000000
```

Debugging Load Balancing

To debug load balancing, use the following commands:

- **debug cable load-balance** *error*
- **debug cable interface**
- **debug cable dcc**
- **debug cable dbc**
- **debug cable mac-address**

Note Use these commands only when you debug load balancing.

Extended Load Balance Debugging

There are different levels of debugging on the load balancing module.

- **debug cable load-balance docsis-lb**

  This command displays debugging messages for load balancing operations on the router.

- **debug cable load-balance docsis-lb lb_docsis_group_id** *docsis-load-balance-group-number* **error**

  This command displays all load balancing debug messages under this load balancing group. The DOCSIS load balancing group can be either a general load balancing group or restricted load balancing group.

- **debug cable load-balance docsis-lb lb_docsis_group_id** *docsis-load-balance-group-number* **assignment**

  This command displays debug messages for CMs added to assignment list.

- **debug cable load-balance docsis-lb lb_docsis_group_id** *docsis-load-balance-group-number* **pending-list**

  This command displays debug messages for the CMs in the pending list.

To test DBC for load balancing, use the following command:

test cable dbc [*ip-address* | *mac-address*]

Configuration Examples for Load Balancing

This section provides the following configuration examples:

Example: Load Balancing Group (Static Load Balancing)

This sample configuration shows a number of load balancing groups being configured for static load balancing operations, with at least one example for each method of calculating the load on an interface.

```
cable load-balance group 1 method modem
cable load-balance group 2 method service-flows
cable load-balance group 3 method utilization
cable load-balance group 3 threshold load 20
cable load-balance group 3 interval 30
cable load-balance group 5 method modem
cable load-balance group 5 threshold load 20
cable load-balance group 5 threshold ugs 60
cable load-balance group 5 policy ugs
cable load-balance group 10 method service-flows
cable load-balance group 10 threshold load 10
```

Example: Load Balancing Group (Passive Load Balancing)

This sample configuration shows a number of load balancing groups being configured for static load balancing operations. The **cable load-balance exclude** command marks a number of cable modems for passive load balancing, while excluding them from static load balancing operations.

```
cable load-balance group 1 method modem
cable load-balance group 2 method service-flows
cable load-balance group 3 method utilization
cable load-balance group 3 threshold load 20
cable load-balance group 3 interval 30
cable load-balance group 5 method modem
cable load-balance group 5 threshold load 20
cable load-balance group 5 threshold ugs 60
cable load-balance group 5 policy ugs
cable load-balance group 10 method service-flows
cable load-balance group 10 threshold load 10
!
cable load-balance exclude oui 00.04.00
cable load-balance exclude oui 00.03.00 static
cable load-balance exclude oui 0C.00.00
cable load-balance exclude modem 0001.0203.0405 static
cable load-balance exclude modem 0C0B.0A09.0807
```

Example: Load Balancing Group (Dynamic Load Balancing)

This sample configuration shows a number of load balancing groups being configured for dynamic load balancing operations.

```
cable load-balance group 1 method modem
cable load-balance group 1 threshold load 20 enforce 20
cable load-balance group 2 method service-flows
cable load-balance group 2 threshold load 10 enforce 10
cable load-balance group 3 method utilization
cable load-balance group 3 threshold load 20 enforce 40
cable load-balance group 3 interval 30
cable load-balance group 5 method modem
cable load-balance group 5 threshold load 20 enforce 25
cable load-balance group 5 threshold ugs 60
cable load-balance group 5 policy ugs
cable load-balance group 10 method service-flows
cable load-balance group 10 threshold load 10 enforce 10
```

Example: Interface Configuration

This sample configuration for a cable interface shows a downstream and its four upstreams being assigned to the same load balancing group:

```
interface Cable3/0
 ip address 10.10.71.1 255.255.255.0
 ip helper-address 10.10.71.1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 8000000
 cable upstream 0 channel-width 200000
 cable upstream 0 minislot-size 64
 cable upstream 0 load-balance group 1
 no cable upstream 0 shutdown
 cable upstream 1 frequency 30000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 load-balance group 1
 no cable upstream 1 shutdown
 cable upstream 2 frequency 22000000
 cable upstream 2 power-level 0
 cable upstream 2 load-balance group 1
 no cable upstream 2 shutdown
 cable upstream 3 frequency 15008000
 cable upstream 3 power-level 0
 cable upstream 3 load-balance group 1
 no cable upstream 3 shutdown
 cable load-balance group 1
```

Note Interface configuration is not required for DOCSIS 3.0 static modem count-based load balancing.

Example: Configuration for Upstreams and Downstreams

The following example shows the configuration necessary to create the load balancing groups that are shown in Figure 6: Example of Load Balancing Groups, on page 427, with load balancing group 1 being used for the two downstreams, load balancing group 2 being used for six upstreams, and load balancing group 3 being used for the remaining two upstreams.

```
! Load-balance group for the two downstreams
cable load-balance group 1 threshold load 10 enforce 20
! Load-balance group for the first six upstreams
cable load-balance group 2 threshold load 10 enforce 20
! Load-balance group for the last two upstreams
cable load-balance group 3 threshold load 10 enforce 20
!
interface Cable5/0
 ip address 11.1.0.1 255.255.0.0 secondary
 ip address 1.2.3.1 255.255.255.0
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 1
 cable upstream 0 frequency 15000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot 4
 cable upstream 0 load-balance group 2
```

```
 no cable upstream 0 shutdown
 cable upstream 1 frequency 18200000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot 4
 cable upstream 1 load-balance group 2
 no cable upstream 1 shutdown
 cable upstream 2 frequency 21400000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot 4
 cable upstream 2 load-balance group 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 24600000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot 4
 cable upstream 3 load-balance group 2
 no cable upstream 3 shutdown
 cable load-balance group 1
 cable dhcp-giaddr policy
interface Cable5/1
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 cable downstream channel-id 2
 cable upstream 0 frequency 29000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot 4
 cable upstream 0 load-balance group 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 32200000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot 4
 cable upstream 1 load-balance group 2
 no cable upstream 1 shutdown
 cable upstream 2 frequency 29000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot 4
 cable upstream 2 load-balance group 3
 no cable upstream 2 shutdown
 cable upstream 3 frequency 32200000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot 4
 cable upstream 3 load-balance group 3
 no cable upstream 3 shutdown
 cable load-balance group 1
 cable dhcp-giaddr policy
```

For DOCSIS 3.0 static modem count-based load balancing, load balancing need not be configured for downstream/upstream under the MAC domain.

The following example shows how to configure the downstream and upstream for the MAC domain:

```
!
interface Cable6/1/0
 downstream Modular-Cable 6/1/0 rf-channel 0-7
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 1
  upstream 0
  upstream 1
  attributes 80000000
 cable upstream bonding-group 2
```

```
  upstream 2
  upstream 3
  attributes 80000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 31600000
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 33200000
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 34800000
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 36400000
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 no cable upstream 3 shutdown
end

cable load-balance docsis-group 3
 downstream Modular-Cable 6/1/0 rf-channel 0-7
 upstream Cable6/1/0 0-3
 threshold load 1
 threshold load minimum 1
 init-tech-list 1-4
!
```

Example: Configuring Dynamic Channel Change for Load Balancing

The following example of the running configuration illustrates DCC for load balancing.

```
Router# show cable load all

*Nov 11 15:42:18.955: %SYS-5-CONFIG_I: Configured from console by conscable load all
Group  Interval  Method      DCC Init     Threshold
                           Technique    Minimum  Static  Enforce  Ugs   PCMM
1      10        modems      0             5        10%     ---     ---   ---

Current load:

Interface            State      Group Utilization  Reserved Modems Flows Weight
Cable3/0 (0 MHz)     initial    1     0%(0%/0%)    0%       0      0     26

Target assignments:

Interface            State      Group  Target
Cable3/0 (0 MHz)     initial    1

Statistics:

Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable3/0 (0 MHz)       initial    0         0         0         0
```

```
Pending:
Modem          Group  Source interface  Target interface     Retries
```

The following example of the running configuration illustrates DCC for load balancing.

```
Router# show running configuration

Building configuration...
Current configuration : 11889 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$tEvV$8xICVVbFm10hx0hAB7DO90
enable password lab
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable load-balance group 1 threshold load 75 enforce
cable load-balance group 1 threshold stability 75
cable load-balance group 1 policy ugs
cable load-balance group 1 threshold ugs 75
cable load-balance group 1 policy pcmm
cable load-balance group 1 threshold pcmm 75
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!
interface GigabitEthernet0/1
 ip address 10.14.1.130 255.255.0.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
```

The following example of the show cable load all command illustrates DCC for load balancing.

```
Router# show cable load all

*Nov 11 15:43:39.979: %SYS-5-CONFIG_I: Configured fromconf t
Group  Interval  Method      DCC Init     Threshold
                             Technique    Minimum  Static  Enforce  Ugs   PCMM
1      10        modems      0             5        75%     75%     75%   75%

Current load:

Interface            State      Group Utilization  Reserved Modems Flows Weight
Cable3/0 (0 MHz)     initial    1     0%(0%/0%)    0%       0      0     26

Target assignments:

Interface            State      Group  Target
Cable3/0 (0 MHz)     initial    1

Statistics:

Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
```

```
Cable3/0 (0 MHz)       initial    0         0         0         0

Pending:

Modem          Group  Source interface  Target interface     Retries
```

The following example illustrates a DCC load balancing group with the default DCC initialization technique. This command configures load balancing group 1:

```
Router(config)# cable load-balance group 1 threshold load 10 enforce
```

This configuration creates a dynamic load balancing group with the following default settings:

```
cable load-balance group 1 method modem
cable load-balance group 1 threshold load 10 enforce
cable load-balance group 1 interval 10
cable load-balance group 1 dcc-init-technique 0
```

The following example changes this DCC load balancing configuration to initialization technique 4:

```
Router# cable load-balance group 1 dcc-init-technique 4
```

Note By default, UGS and PCMM policies are not turned on, so that CMs with active voice calls or PCMM calls participate in load balancing.

Additional References

For additional information related to Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS, see the following references:

Related Documents

Related Topic	Document Title
Cable commands	Cisco IOS CMTS Cable Command Reference, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/ cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/ prod_command_reference_list.html

Standards and RFCs

Standard/RFC[29]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

Standard/RFC[29]	Title
RFC 1163	Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2233	DOCSIS OSSI Objects Support
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

29 Not all supported standards and RFCs are listed.

MIBs

MIBs[30]	MIBs Link
New MIBs are introduced in Cisco IOS Release 12.3(17a)BC in support of DCC for load balancing. • docsQosDCCReqs OBJECT-TYPE • docsQosDCCRsps OBJECT-TYPE • docsQosDCCAcks OBJECT-TYPE • docsQosDCCs OBJECT-TYPE • docsQosDCCFails OBJECT-TYPE	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

30 Not all supported MIBs are listed.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 41: Feature Information for Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers

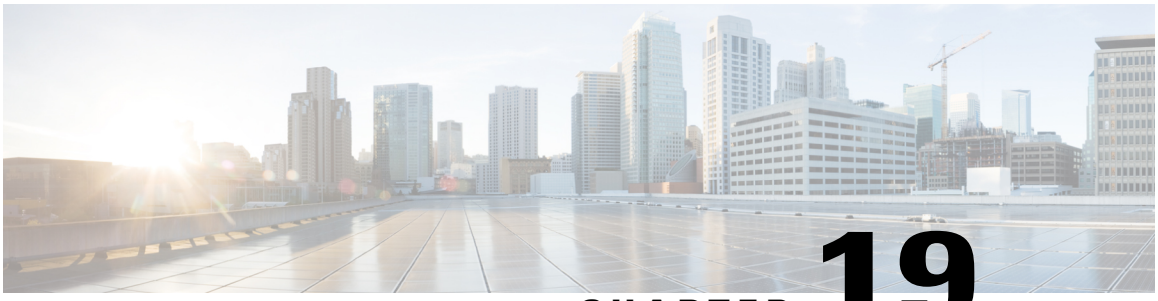
Feature Name	Releases	Feature Information
Load Balancing on the Cisco CMTS Routers	12.2(15)BC1	This feature was introduced on the Cisco uBR10012 and Cisco uBR7246VXR Universal Broadband Routers. The following commands were introduced: **cable load-balance exclude** , **cable load-balance group (global configuration)**, **cable load-balance group (interface)** , **cable load-balance group interval**, **cable load-balance group policy ugs**, **cable load-balance group threshold**, **cable upstream load-balance group**, **clear cable load-balance**, **debug cable load-balance**, **show cable load-balance**, **test cable load-balance**
Load Balancing on the Cisco CMTS Routers	12.3(9a)BC	This feature was introduced on the Cisco uBR7100 Series Universal Broadband Routers.

Feature Name	Releases	Feature Information
Dynamic Channel Change (DCC) for Load Balancing on the Cisco CMTS Routers	12.3(17a)BC	This feature was introduced on the Cisco uBR10012 and Cisco uBR7246VXR Universal Broadband Routers. The following commands were introduced or modified: **cable load-balance group dcc-init-technique** , **cable load-balance group policy**, **cable load-balance group threshold**, **show controllers cable**, **test cable dcc**
Enhancements to Downstream Load Balancing on the Cisco CMTS Routers	12.3(17b)BC4	Downstream load balancing is further enhanced to equalize downstream load balancing with upstream load balancing group members. The following commands were modified: **cable load-balance group policy** , **show cable load-balance all**
Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.
Load balancing Prohibition Based on Group Policy ID	12.2(33)SCB	Load balancing is further enhanced with the addition of rules and policies. The following commands were added: **cable load-balance rule**, **cable load-balance docsis-policy**
Upstream Load Balancing for DOCSIS 3.0 Cable Modems in Single Upstream Mode	12.2(33)SCC	The upstream load balancing functionality enables the Cisco uBR10012 router to effectively handle upstream traffic for wideband and narrowband cable modems that are in single upstream mode.

Feature Name	Releases	Feature Information
DOCSIS 2.0 multicast enhancement for VDOC.	12.2(33)SCD5	This feature enables the customer to tune a DOCSIS 2.0 cable modem to a specific downstream and supports static multicast video forwarding on it. The following command was modified: • **cable load-balance rule**
Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers	12.2(33)SCE	This feature was integrated into Cisco IOS Release 12.2(33)SCE.
Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers	12.2(33)SCF	The error handling of channel assignment was modified. The Service Flows method was deprecated.
Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers	12.2(33)SCE4	Support for 256 legacy LBGs was added. The following commands are modified: • **cable load-balance group** • **cable load-balance group (interface)** • **cable load-balance group interval** • **cable load-balance group policy ugs** • **cable load-balance group threshold** • **cable upstream load-balance group** • **show cable load-balance**
Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers	12.2(33)SCF1	DBC was added to the load balancing feature.

Feature Name	Releases	Feature Information
Display Status Information of modems in a Load Balancing Group	12.2(33)SCH	The output of the following command is modified to display the status of the modems in a Load Balancing Group: **show cable load-balance docsis-group**
Default settings for D3.0 and D2.0 GLBG	12.2(33)SCH	Support for additional default configuration settings for DOCSIS 3.0 and DOCSIS 2.0 GLBGs. The following commands are modified: **cable load-balance d30-ggrp-default**, **cable load-balance d20-ggrp-default**
Minimum Threshold under Utilization Method	12.2(33)SCH	Support for configuring minimum threshold for load balancing under Utilization method was added. The following new command was introduced: **cable load-balance method-utilization min-threshold**
Support for Excluding Old Devices	12.2(33)SCH	Support for Exclusion of Old Devices using Address Mask and in Assignment Phase The following command was modified: **cable load-balance exclude**
Primary Channel Load Display for Target RCS	12.2(33)SCH	Support for primary channel load-based RCS selection for DOCSIS 3.0 static load balancing. The following command was modified: **show cable load-balance docsis-group**

Feature Name	Releases	Feature Information
Disabling Upstream Load Balancing for DOCSIS 3.0 Modems	12.2(33)SCH1 12.2(33)SCG6	Support for activating load balancing only on downstream channels. The following commands are modified: • **cable load-balance docsis30-enable** • **show cable load-balance** For more information, see Disabling Upstream Load Balancing for DOCSIS 3.0 Modems, on page 429.
D30 Dynamic Load Balancing	12.2(33)SCI	Support for activating the DOCSIS 3.0 dynamic load balancing on the downstream channels. The following commands are introduced or modified: • **cable load-balance docsis30-dynamic-enable** • **clear cable load-balance error-statistics** • **show cable load-balance docsis-group** • **show cable load-balance statistics** For more information, see DOCSIS 3.0 Dynamic Load Balancing, on page 430.



CHAPTER 19

M-CMTS DEPI Control Plane

First Published: November 16, 2009

Last Updated: September 17, 2012

The Downstream External PHY Interface (DEPI) control plane feature is based upon Layer Two Tunneling Protocol-Version 3 (L2TPv3) signaling. Downstream External PHY Interface is a communication protocol between the Modular Cable Modem Termination System (M-CMTS) core and the Edge Quadrature Amplitude Modulation (EQAM). It is an IP tunnel between the MAC (M-CMTS Core) and PHY (EQAM) in an M-CMTS system, which contains both a data path for Data-Over-Cable Service Interface Specifications (DOCSIS) frames and a control path for setting up, maintaining, and tearing down data sessions.

The DEPI Latency Measurement (DLM) packet is a special type of data packet used for measuring the network latency between the M-CMTS core and the EQAM. There are two types of DLM packets, ingress DLM packet and egress DLM packet. The ingress DLM measures the latency between the M-CMTS core and the ingress point in the EQAM, and the egress DLM measures the latency between the M-CMTS core and the egress point of the EQAM. The DEPI Control Plane is supported with a direct connection between the SPA and the EQAM, or between the Cisco uBR-MC3GX60V line card and the EQAM.

The Converged Interconnect Network (CIN) is the standard term used for the network between the M-CMTS and the Radio Frequency Gateway (RFGW). This network can be a direct connection or a Layer 2 or Layer 3 network. Since the CIN is a private network, a Virtual Routing and Forwarding (VRF) instance ensures that only valid traffic is routed to it by removing the IP Address of the interface from the global routing table (and from the interface).

Note Layer 3 CIN support is limited to the case where the primary GigE link of the M-CMTS DEPI port is connected directly to the EQAM and the secondary link is connected through a Layer 3 router. The Layer 3 router between the M-CMTS and the EQAM must support modifying the MAC addresses on its Layer 3 interface.

VRF for DEPI session is used only on the M-CMTS router. It is recommended to configure VRF for the GigE interfaces, to ensure that the CIN routes are isolated from the default routing table of the CMTS router. When connecting two SPAs to a Layer 2 CIN, the GigE interfaces for these SPAs need to be configured with different VRFs.

PortFast mode-enabled switches have to be used when Gigabit Ethernet link redundancy is configured for the Gigabit Ethernet (GigE) interfaces. For more information on the switches that support PortFast mode, see

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for M-CMTS DEPI Control Plane

The following are the prerequisites for the M-CMTS DEPI Control Plane feature:

- Support of bidirectional communication using the GigE ports on the Cisco Wideband SPA or Cisco uBR-MC3GX60V line card.
- Support DLM (Ingress).
- Support of EQAM configuration from the M-CMTS router (with EQAM in learn mode). The learn feature is supported only on Cisco RFGW-10.
- Provide connectivity verification, and link failure detection.
- Support Management Information Base (MIB).

The table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 42: Cable Hardware Compatibility Matrix for M-CMTS DEPI Control Plane

Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCC and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCC and later releases • Cisco Wideband SPA Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[31]

31 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

Restrictions for M-CMTS DEPI Control Plane

- Supports only DOCSIS MPEG-TS (DMPT) mode.
- Modular QoS CLI (MQC) or access control lists (ACL) related features are *not* supported on the DEPI interface.
- The IP address of the DEPI interface must be configured manually. It *cannot* be assigned by the DHCP server.
- VLAN subinterfaces are *not* supported only on the following:
  - Cisco uBR-MC3GX60V line card
  - Cisco Wideband SPA
- Secondary IP address are *not* supported on the DEPI interface.
- Mixed DEPI configuration of manual DEPI and remote DEPI is *not* permitted on the same Cisco uBR-MC3GX60V line card or the Cisco Wideband SPA.
- Configuring or removing an IP address on the controller is *not* permitted when the DEPI interface with an IP address exists in manual DEPI configuration.
- Configuring an IP address on the controller is not permitted in remote DEPI configuration.

Information About M-CMTS DEPI Control Plane

To configure the M-CMTS DEPI Control Plane feature, you should understand the following concepts:

Benefits of M-CMTS DEPI Control Plane

- The DEPI control plane provides the capability to detect failures in a multi-hop network between the M-CMTS router and EQAM.
- The Cisco RFGW-10 (EQAM) learns the configuration from the M-CMTS router via the DEPI control plane.
- The DEPI control plane facilitates an automatic and accurate method to determine delay via the DLM.
- The DEPI control plane allows interoperability.

DEPI Control Connections

The DEPI control plane configuration is possible only with the following devices that have GigE ports:

- Cisco Wideband SPA—Cisco IOS Release 12.2(33)SCC and later releases
- Cisco uBR-MC3GX60 line card—Cisco IOS Release 12.2(33)SCE and later releases

Configuring a DEPI tunnel on a SPA or Cisco uBR-MC3GX60 line card downstream channel will establish a DEPI control connection (if it does not exist). The M-CMTS router (not the EQAM) initiates the control session connection. At least one DEPI control connection must exist for each SPA or Cisco uBR-MC3GX60 line card that has RF channels configured, to establish a DEPI session with an EQAM. There can be multiple control connections from one SPA or Cisco uBR-MC3GX60 line card to one or more EQAMs. When a DEPI control connection is disconnected, all the associated DEPI data sessions will be disconnected.

When the primary link on the SPA or Cisco uBR-MC3GX60 line card toggles more than five times within 30 seconds, and the secondary link is up, the secondary link is selected for traffic. The link switches back to the primary link during the next primary link transition after 30 seconds or when the secondary link fails. To get the primary link (port 0) or secondary link (port 1) status, use the **show controller gigabitethernet** command.

DEPI Data Sessions

For both primary and non-primary downstream channels, the DEPI data session is established when the DEPI control connection is active. The Transport Stream Identifier (TSID) must be configured on both the M-CMTS router and EQAM, as it is used to bind the logical wideband channel to a physical QAM of the EQAM. Only the M-CMTS router initiates the DEPI data session creation, not the EQAM.

DEPI SSO

The Cisco RFGW-10 supervisor redundancy and the route processor (RP) redundancy on the Cisco uBR10012 router in stateful switchover (SSO) mode support both DEPI manual mode and DEPI protocol mode (control plane DEPI). Minimal disruption might occur in manual DEPI in the case of RP redundancy on the Cisco uBR10012 router. The control plane and data sessions are reestablished after the RP switchover in control plane DEPI while the data plane non-stop forwarding continues to send DEPI data traffic to the EQAM.

With supervisor redundancy, the supervisor switchover does not affect the statically configured DEPI connections in DEPI manual mode. Hence, the switchover interruption to DEPI data traffic is in subseconds. In DEPI protocol mode, the DEPI control plane is SSO-unaware as the underlying IOS L2TPv3 protocol is SSO-unaware. Neither the L2TPv3 protocol state nor the DEPI state is check pointed from the active Supervisor

to the standby Supervisor. During Supervisor switchover, the DEPI control plane and data plane are recovered as follows with minimal service outage time:

- DEPI control plane and data plane re-establishment: At Supervisor switchover, the newly active Supervisor card re-establishes the DEPI control connections and data sessions with its M-CMTS peer. The IDs of re-established sessions fall into the same DEPI session ID range as before.
- DEPI data plane non-stop forwarding: While the newly active Supervisor is re-establishing the DEPI connections and data sessions, the Cisco RFGW-10 receives and processes DEPI data traffic that the M-CMTS router continues to forward through the existing data sessions. This non-stop forwarding function minimizes the service outage time for a couple of seconds. The existing data sessions are removed after the new sessions are established.

For more information on Supervisor Redundancy, see 1:1 Supervisor Card Redundancy feature guide.

N+1 DEPI Redundancy

The N+1 DEPI redundancy feature enables the M-CMTS router to protect downstream data path in the event of the Cisco uBR-MC3GX60V line card failure or switchover, using a secondary DEPI session configured on the protect line card. Beginning with Cisco IOS Release 12.2(33)SCE1, the N+1 redundancy feature including DEPI redundancy is supported on the Cisco uBR-MC3GX60V cable interface line card.

This feature allows you to configure a secondary DEPI session on the protect card using the **protect-tunnel** command in DEPI tunnel configuration mode. In this mode, the protect line card has a fully operational secondary DEPI control connection and sessions for the QAM channels on the working line card. The primary DEPI control connection and session is established on the GigE ports on the working line card. These primary and secondary DEPI sessions are paired using the common TSID, which uniquely identifies the target QAM channel.

The N+1 DEPI redundancy feature is supported only on the Cisco uBR-MC3GX60 line card. This feature is not supported on the Cisco Wideband SPA.

The N+1 DEPI redundancy feature requires an EQAM that supports data path redundancy based on CableLabs Downstream External PHY Interface Specification (CM-SP-DEPI-I08-100611).

The Cisco uBR-MC3GX60V line card supports up to six DEPI tunnels per GigE port and a separate DEPI session per downstream channel. Each DEPI session is associated with only one DEPI tunnel and multiple DEPI sessions can be associated with a single DEPI tunnel.

In N+1 DEPI redundancy, the protect line card initiates DEPI control sessions on each QAM channel at bootup. When the M-CMTS router detects a line card failure, the protect line card enables all the sessions that were backing up the sessions of the failed line card.

The network connectivity must be set up to ensure that the Cisco RF Gateway is reachable through the protect Cisco uBR-MC3GX60V line card.

DEPI CIN Failover

The **depi cin-failover** command is introduced to enable CIN failure triggered line card switchover when DEPI control plane is used and N+1 is configured.

When the CPU utilization is high, DEPI CIN failover may get rejected. Starting Cisco IOS Release 12.2(33)SCF4 and later releases, **cpu-thresold** values can be configured using the **depi cin-faiover cpu-threshold** command. For more information, see Cisco IOS CMTS Cable Command Reference.

Downstream Failure Detection

The control plane DEPI detects the downstream device or connection failure on the Cisco uBR-MC3GX60V line card using the “hello” keepalive packets. It triggers the line card switchover if the protect line card DEPI sessions are the superset of the working line card. You can configure the interval used to exchange the “hello” keepalive packets in a Layer 2 control channel using the **hello** command in L2TP class configuration mode.

GigE Port-level Redundancy

The Cisco uBR-MC3GX60V line card also supports GigE port-level redundancy. The port-level redundancy is configured by default on the Cisco Wideband SPA and Cisco uBR-MC3GX60V line card. You do not have to manually configure port-level redundancy on the M-CMTS router.

Difference Between Manual DEPI and Control Plane DEPI Configuration

The manual DEPI configuration also supports N+1 DEPI redundancy and port-level redundancy on the Cisco uBR-MC3GX60V line card.

The following are the differences between the manual DEPI and control plane DEPI configuration:

- In manual DEPI configuration, you do not have to configure the protect tunnel. The working card configuration is automatically applied to the protect card through IPC messages. In DEPI control plane redundancy, you must configure the protect tunnel on both the M-CMTS router and the EQAM.
- For manual DEPI configuration, the GigE ports on the Cisco uBR-MC3GX60V line card must be in active-passive mode.
- The DEPI connection between the M-CMTS router and the EQAM is static in manual DEPI configuration. Whereas, the data sessions are established dynamically in the DEPI control plane configuration.

DEPI EQAM Statistics

The DEPI EQAM statistics feature enables EQAM to send QAM channel statistics to the M-CMTS router for all data sessions in every DEPI tunnel. Support for this feature was introduced in Cisco IOS Release 12.2(33)SCE. The DEPI EQAM statistics feature is configured by default on the M-CMTS router. To disable this configuration use the **no** form of the **depi eqam-stats** command in global configuration mode.

Note Cisco RF Gateway 10 sends EQAM statistics to the M-CMTS router. No other EQAM supports the EQAM statistics feature.

To verify EQAM statistics, use the **show depi session** command with the **verbose** keyword in privileged EXEC mode.

How to Configure M-CMTS DEPI Control Plane

For a quick tour on how to configure DEPI on the Cisco M-CMTS router and the EQAM device, view the following videos available on Cisco.com:

- Configuring the Downstream External PHY Interface Feature on the Cisco M-CMTS and EQAM Device [Part 1 of 2]

- Configuring the Downstream External PHY Interface Feature on the Cisco M-CMTS and EQAM Device [Part 2 of 2]

This section contains the following procedures:

Configuring DEPI Control Plane on the M-CMTS Router

This section describes how to configure DEPI control plane on the M-CMTS router.

Note The DEPI control plane configuration steps for the Cisco Wideband SPA and Cisco uBR-MC3GX60 line card are the same. Step 17, on page 471 is applicable only for the Cisco Wideband SPA and is not required for Cisco uBR-MC3GX60 line card.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2tp-class l2tp-class-name** **Example:** `Router(config)# l2tp-class class1`	Creates an L2TP class template. The template must be configured but the optional settings are not mandatory. **Note** If all the control channels have the same parameters then a separate template must be created for the M-CMTS.
Step 4	**hello** *seconds* **Example:** `Router(config-l2tp-class)# hello 5`	(Optional) Configures the interval used to exchange the “hello” keepalive packets in a Layer 2 control channel. • *seconds*—Number of seconds that a router at one end of a Layer 2 control channel waits between sending the “hello” keepalive packets to its peer router. The valid range is from 0 to 1000 seconds. The default value is 60 seconds. **Note** If you want the DEPI tunnel to be less sensitive to network disturbances, increase the interval for the “hello” keepalive packets. We recommend that you specify 5 seconds on the M-CMTS router.
Step 5	**retransmit retries** *max-retransmissions* **Example:** `Router(config-l2tp-class)# retransmit retries 5`	(Optional) Configures the retransmission retry settings of the control packets. • *max-retransmissions*—Number of retransmission cycles that occur before determining that the peer provider edge (PE) router does not respond. The valid range is from 5 to 1000. The default value is 15. Specify a smaller value for faster failure detection.

	Command or Action	Purpose
		Note We recommend that you specify 5 on the M-CMTS router.
Step 6	**retransmit timeout** {**max** | **min**} *retransmit-timeout* **Example:** `Router(config-l2tp-class)# retransmit timeout max 1`	Specifies maximum and minimum retransmission intervals (in seconds) for resending the control packets. • {**max** | **min**} *retransmit-timeout*—The valid range is from 1 to 8. The default maximum interval is 8; the default minimum interval is 1. **Note** We recommend that you specify 1 second on the M-CMTS router.
Step 7	**exit** **Example:** `Router(config-l2tp-class)# exit`	Exits the L2TP class configuration mode.
Step 8	**depi-class** *depi-class-name* **Example:** `Router(config)# depi-class SPA0`	Creates a DEPI class template.
Step 9	**exit** **Example:** `Router(config-depi-class)# exit`	Exits the DEPI class configuration mode.
Step 10	**depi-tunnel** *working-depi-tunnel-name* **Example:** `Router(config)# depi-tunnel SPA0`	Creates a DEPI tunnel template.
Step 11	**l2tp-class** *l2tp-class-name* **Example:** `Router(config-depi-tunnel)# l2tp-class class1`	Specifies the L2TP control channel parameters to be inherited.
Step 12	**depi-class** *depi-class-name* **Example:** `Router(config-depi-tunnel)# depi-class SPA0`	Specifies the DEPI control channel parameters to be inherited.
Step 13	**dest-ip** *dest-ip-address* **Example:** `Router(config-depi-tunnel)# dest-ip 192.0.2.103`	Specifies the destination IP address of the termination point for the DEPI tunnel. When configuring on the M-CMTS router, destination IP address is the IP address of the EQAM. When configuring on the EQAM, this is the IP address of the M-CMTS router.
Step 14	**tos** *value* **Example:** `Router(config-depi-tunnel)# tos 100`	(Optional) Sets the value of the ToS byte for IP packets in the L2TPv3 data session. The valid range is from 0 to 255. The default value is 0.

	Command or Action	Purpose
Step 15	**exit** **Example:** `Router(config-depi-tunnel)# exit`	Exits the data session configuration mode.
Step 16	**controller modular-cable** {*slot*/*bay*/*port* | *slot*/*subslot*/*controller*} **Example:** `Router(config)# controller modular-cable 1/0/0`	Specifies the modular cable controller interface for the SPA or the line card. • *slot*—SPA interface processor (SIP) or the line card slot. Slots 1 and 3 are used for SIPs. The valid range is from 5 to 8 for the line card slot. • *bay*—The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). • *port*—Specifies the interface number on the SPA. • *subslot*—Cable interface line card subslot. Valid values are 0 and 1. • *controller*—Controller index for the modular cable. The valid range is from 0 to 2.
Step 17	**modular-host subslot** *slot/subslot* **Example:** `Router(config-controller)# modular-host subslot 6/0`	Specifies the modular host line card that is used for DOCSIS 3.0 downstream or downstream channel bonding operations.
Step 18	**rf-channel** *rf-port* **cable downstream channel-id** *channel-id* **Example:** `Router(config-controller)# rf-channel 0 cable downstream channel-id 24`	Assigns a downstream channel ID to an RF channel. • *rf-port*—RF channel physical port on the SPA or the line card. Valid values for the RF port depend on the configuration of the annex modulation. • *channel-id*—Unique channel ID. The valid range is from 1 to 255.
Step 19	**rf-channel** *rf-port* **frequency** [*freq* | **none**] [**annex** {**A** | B} **modulation** {**64** | **256**} [**interleave-depth** {**8** | **12** | **16** | **32** | **64** | **128**}]] **Example:** `Router(config-controller)# rf-channel 0 freq 555000000 annex B mod 64qam inter 32`	Configures the frequency of an RF channel in modular cable controller configuration mode. • *rf-port*—RF channel physical port on the SPA or the line card. Valid values for the RF port depend on the configuration of the annex modulation. • *freq*—Center frequency of the RF channel. The valid range for each RF channel is different based on the Annex type. • **none**—Removes the specified frequency if the RF channel is shut down. This can be configured on the modular cable controller of the N+1 protect line card as no frequency is required to be configured on that controller. • **annex** {**A** | **B**}—Indicates the MPEG framing format for each RF channel.

	Command or Action	Purpose
		◦ **A—**Annex A. Indicates that the downstream is compatible with the European MPEG framing format specified in ITU-TJ.83 Annex A. ◦ **B—**Annex B. Indicates that the downstream is compatible with the North American MPEG framing format specified in ITU-TJ.83 Annex B. • **modulation** {**64** | **256**}**—**Indicates the modulation rate (64 or 256 QAM) for each RF channel. • **interleave-depth—**Indicates the downstream interleave depth. For annex A, the interleave value is 12. For annex B, valid values are 8, 16, 32, 64, and 128.
Step 20	**rf-channel** *rf-channel* **depi-tunnel** *depi-tunnel-name* **tsid** *id* **Example:** `Router(config-controller)# rf-channel 0 depi-tunnel SPA0 tsid 100`	Binds the DEPI tunnel, which inherits the configuration of the specified L2TP class and DEPI class, to an RF channel under a modular controller. • *rf-channel***—**RF channel physical port on the SPA or the line card. • *depi-tunnel-name***—**Name of the DEPI tunnel. • **tsid** *id***—**Specifies the Transport Stream Identifier (TSID) value on the QAM subinterface. The TSID is used to associate the logical RF channel of the SPA or the line card to a physical QAM on RF Gateway 10.
Step 21	**rf-channel** *rf-port* **rf-power** *power-level* **Example:** `Router(config-controller)# rf-channel 0 rf-power 46`	Configures the RF power of an RF channel on the SPA or the line card. • *rf-port***—**RF channel physical port on the SPA or the line card. Valid values for the RF port depend on the configuration of the annex modulation. • *power-level***—**Desired RF output power level in dBmV. The valid range is dependent on the cable interface. The format is XY.Z. By default, .Z is added as .0.
Step 22	**no rf-channel** *rf-port* **rf-shutdown** **Example:** `Router(config-controller)# no rf-channel 0 rf-shutdown`	Enables the RF channel. • *rf-port***—**RF channel physical port on the SPA or the line card. Valid values for the RF port depend on the configuration of the annex modulation.
Step 23	**exit** **Example:** `Router(config-controller)# exit`	Exits the controller configuration mode.

	Command or Action	Purpose
Step 24	**interface gigabitethernet** *slot/subslot/port* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Specifies the location of the Gigabit Ethernet interface on the M-CMTS router. • *slot*—SPA interface processor (SIP) or the line card slot. Slots 1 and 3 are used for SIPs. The valid range is from 5 to 8 for the line card slot. • *subslot*—Specifies the secondary slot of the SIP where the SPA is installed or the c*able interface line card subslot. Valid values are 0 and 1*. • *port*—Specifies the interface number.
Step 25	**ip-address** *ip-address mask-ip-address* **Example:** `Router(config-if)# ip-address 192.0.2.155 255.255.255.0`	Sets the IP address for the SPA or the line card field-programmable gate array (FPGA). This address is used as the source IP address for packets that the router transmits to the EQAM device.
Step 26	**negotiation** {**forced** | **auto**} **Example:** `Router(config-if)# negotiation auto`	Enables negotiation on the SPA or the line card interface.
Step 27	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring DEPI Control Plane on Cisco RFGW-10

This section describes how to configure DEPI control plane on Cisco RFGW-10 in learn mode. Learn mode is the recommended mode of operation if you use Cisco RFGW-10 with the Cisco uBR10012 router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**l2tp-class** *l2tp-class-name* **Example:** `Router(config)# l2tp-class class1`	Creates an L2TP class template. The template must be configured but the optional settings are not mandatory. **Note** If all the control channels have the same parameters then one template must be created for the Cisco RFGW-10.
Step 4	**hello** *seconds* **Example:** `Router(config-l2tp-class)# hello 15`	(Optional) Configures the interval used to exchange the "hello" keepalive packets in a Layer 2 control channel. • *seconds*—Number of seconds that a router at one end of a Layer 2 control channel waits between sending the "hello" keepalive packets to its peer router. The valid range is from 0 to 1000 seconds. The default value is 60 seconds. **Note** The "hello" value on the Cisco RFGW-10 can be different from what is configured on the M-CMTS router. We recommend that you specify 15 seconds on the Cisco RFGW-10. A value of less than 10 seconds might subject the system to session flaps and may trigger line card switchover, if the M-CMTS router experiences loss of network connectivity.
Step 5	**retransmit retries** *max-retransmissions* **Example:** `Router(config-l2tp-class)# retransmit retries 5`	(Optional) Configures the retransmission retry settings of the control packets. • *max-retransmissions*—Number of retransmission cycles that occur before determining that the peer provider edge (PE) router does not respond. The valid range is from 5 to 1000. The default value is 15. Specify a smaller value for faster failure detection. **Note** We recommend that you specify 5 on the Cisco RFGW-10.
Step 6	**retransmit timeout** [**max** | **min**] *retransmit-timeout* **Example:** `Router(config-l2tp-class)# retransmit timeout max 1`	Specifies maximum and minimum retransmission intervals (in seconds) for resending the control packets. • {**max** | **min**} *retransmit-timeout*—The valid range is from 1 to 8. The default maximum interval is 8; the default minimum interval is 1. **Note** We recommend that you specify 1 second on the Cisco RFGW-10.
Step 7	**exit** **Example:** `Router(config-l2tp-class)# exit`	Exits the L2TP class configuration mode.
Step 8	**depi-class** *depi-class-name* **Example:** `Router(config)# depi-class SPA0`	Creates a DEPI class template.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-depi-class)# exit`	Exits the DEPI class configuration mode.
Step 10	**depi-tunnel** *working-depi-tunnel-name* **Example:** `Router(config)# depi-tunnel SPA0`	Creates a DEPI tunnel template.
Step 11	**l2tp-class** *l2tp-class-name* **Example:** `Router(config-depi-tunnel)# l2tp-class class1`	Specifies the L2TP control channel parameters to be inherited.
Step 12	**depi-class** *depi-class-name* **Example:** `Router(config-depi-tunnel)# depi-class SPA0`	Specifies the DEPI control channel parameters to be inherited.
Step 13	**dest-ip** *dest-ip-address* **Example:** `Router(config-depi-tunnel)# dest-ip 192.0.2.155`	Specifies the destination IP address of the M-CMTS Gigabit Ethernet port.
Step 14	**exit** **Example:** `Router(config-depi-tunnel)# exit`	Exits the DEPI configuration mode.
Step 15	**interface** {**qam** | **qam-red**} *slot/port*[*.channel*] **Example:** `Router(config)# interface qam 6/4.1`	Specifies a QAM interface or redundancy-configured (QAM-red) interface. • *slot*—The QAM or QAM-red slot for the line card on Cisco RF Gateway 10. If line card redundancy is configured on the QAM, the interface is QAM-red. The valid range is from 3 to 12. • *port*—Interface number on the line card. The valid range is from 1 to 12. • *.channel*—(Optional) Specifies the channel on the port. The valid range is from 1 to 4.
Step 16	**cable mode** {**depi** | **video**} {**local** | **remote**} [**learn**] **Example:** `Router(config-subif)# cable mode depi remote learn`	Sets the mode of the QAM channel. • **depi**—Specifies the DEPI mode of the QAM channel. • **video**—Specifies the video mode of the QAM channel. • **local**—Specifies that the QAM channel is manually configured. • **remote**—Specifies that the QAM channel is remotely configured.

	Command or Action	Purpose
		• **learn—**(Optional) Specifies that the QAM channel is in "learn" mode and the Cisco RFGW-10 can learn the channel configuration from the M-CMTS router. All QAM channels on a single port must be in "learn" mode for this configuration to work. **Note** When the QAM is in "learn" mode, there is no need to configure all the QAM channel parameters. Step 17, on page 476 to Step 24, on page 477 should not be executed as the parameters in these steps cannot be changed when the Cisco RFGW-10 is in "learn" mode.
Step 17	**cable downstream stacking** *stacking* **Example:** `Router(config)# cable downstream stacking 4`	Configures the stacking level. Stacking level can be 1, 2, or, 4. • QAM channel 1 is enabled on the specified RF port for stacking level 1. • QAM channels 1, and 2 are enabled on the specified RF port for stacking level 2. • QAM channels 1, 2, 3, and 4 are enabled on the specified RF port for stacking level 4.
Step 18	**no cable downstream rf-shutdown** **Example:** `Router(config-if)# no cable downstream rf-shutdown`	Enables the integrated upconverter.
Step 19	**cable downstream annex** {**A** | **B**} **Example:** `Router(config-if)# cable downstream Annex A`	Configures the MPEG framing format for a downstream port. • **annex** {**A** | **B**}**—**Indicates the MPEG framing format for each RF channel. ◦ **A—**Annex A. Indicates that the downstream is compatible with the European MPEG framing format specified in ITU-TJ.83 Annex A. ◦ **B—**Annex B. Indicates that the downstream is compatible with the North American MPEG framing format specified in ITU-TJ.83 Annex B. The default is Annex B for all Cisco cable interface line cards.
Step 20	**cable downstream frequency** *frequency* **Example:** `Router(config-if)# cable downstream frequency 520000000`	Configures the downstream center frequency for the cable interface line card. • *frequency***—**QAM channel frequency in Hz.
Step 21	**cable downstream interleave-level** {**1** | **2**}	Configures the interleave level. The default interleave level is 2.

	Command or Action	Purpose
	Example: `Router(config-subif)# cable downstream interleave-level 1`	**Note** This command is for Annex B only.
Step 22	**cable downstream interleave-depth** *depth* **Example:** `Router(config-subif)# cable downstream interleave-depth 5`	Configures the interleave depth. **Note** This command is for Annex B only. As you can configure various combinations of the I/J values for Annex B, the input for this command is the fee-code that is derived from the I/J values. The default I/J values are 32/4.
Step 23	**cable downstream modulation** {**64qam** | **256qam**} **Example:** `Router(config-subif)# cable downstream modulation 256qam`	Configures the modulation format for a downstream port on a cable interface line card. If you change the modulation format, the interface is shut down and all the cable modems are disconnected. The default modulation is set to 64 QAM on all cable interface cards.
Step 24	**cable downstream rf-power** *power* **Example:** `Router(config-subif)# cable downstream rf-power 50`	Configures the RF power output level on an integrated upconverter. • *power*—RF power value in tenth of a dBmV. To reset the RF output power level to its default value, use the no form of this command.
Step 25	**cable downstream tsid** *id* **Example:** `Router(config-subif)# cable downstream tsid 100`	Configures the Transport Stream Identifier value on the QAM subinterface. The valid range is from 0 to 65535.
Step 26	**depi depi-tunnel** *working-depi-tunnel-name* **Example:** `Router(config-subif)# depi depi-tunnel working1`	Binds the DEPI tunnel to the QAM.
Step 27	**exit** **Example:** `Router(config-subif)# exit`	Exits the subinterface configuration mode. The Cisco RFGW-10 is now ready to accept incoming control connection requests from the M-CMTS router but cannot initiate a control connection with the router.
Step 28	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 6/13`	Specifies the Gigabit Ethernet interface.
Step 29	**no switchport** **Example:** `Router(config-if)# no switchport`	Disables switching mode.

	Command or Action	Purpose
Step 30	**ip-address** *ip-address mask-ip-address* **Example:** `Router(config-if)# ip-address 192.0.2.103 255.255.255.0`	Sets the IP address for the SPA or the line card field-programmable gate array (FPGA). This address is used as the source IP address of Cisco RFGW-10.
Step 31	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Examples

The following is an example for configuring DEPI on Cisco RFGW-10, which is in **learn** mode.

```
Router> enable
Router# configure terminal
Router(config)# l2tp-class class1
Router(config-l2tp-class)# hello 15
Router(config-l2tp-class)# retransmit retries 5
Router(config-l2tp-class)# retransmit timeout max 1
Router(config-l2tp-class)# exit
Router(config)# depi-class 0
Router(config-depi-class)# exit
Router(config)# depi-tunnel 0
Router(config-depi-tunnel)# l2tp-class class1
Router(config-depi-tunnel)# depi-class 0
Router(config-depi-tunnel)# dest-ip 192.0.2.155
Router(config-depi-tunnel)# exit
Router(config)# interface qam 6/4.1
Router(config-subif)# cable mode depi remote learn
Router(config-subif)# cable downstream tsid 100
Router(config-subif)# depi depi-tunnel working1
Router(config-subif)# exit
Router(config)# interface gigabitethernet 6/13
Router(config-if)# no switchport
Router(config-if)# ip-address 192.0.2.103 255.255.255.0
Router(config-if)# end
```

The following is an example for configuring DEPI on Cisco RFGW-10, which is not in “learn” mode.

```
Router> enable
Router# configure terminal
Router(config)# l2tp-class class1
Router(config-l2tp-class)# exit
Router(config)# depi-class 0
Router(config-depi-class)# exit
Router(config)# depi-tunnel 0
Router(config-depi-tunnel)# l2tp-class class1
Router(config-depi-tunnel)# depi-class 0
Router(config-depi-tunnel)# dest-ip 192.0.2.155
Router(config-depi-tunnel)# exit
Router(config)# interface qam 6/4.1
Router(config-subif)# cable mode depi remote learn
Router(config-subif)# cable downstream stacking 4
Router(config-subif)# no cable downstream rf-shutdown
Router(config-subif)# cable downstream Annex B
Router(config-subif)# cable downstream frequency 520000000
Router(config-subif)# cable downstream tsid 100
```

```
Router(config-subif)# cable downstream interleave-level 2
Router(config-subif)# cable downstream interleave-depth 5
Router(config-subif)# cable downstream modulation 256qam
Router(config-subif)# cable downstream rf-power 50
Router(config-subif)# depi depi-tunnel 0
Router(config-subif)# end
```

Configuring N+1 DEPI Redundancy on the M-CMTS Router and Cisco RFGW-10

This configuration is optional. This section describes how to configure N+1 DEPI redundancy on the M-CMTS router and Cisco RFGW-10.

Note The N+1 DEPI redundancy feature is supported only on the Cisco uBR-MC3GX60V line card. This feature is not supported on the Cisco Wideband SPA.

The procedure is the same for configuring N+1 DEPI redundancy on the M-CMTS router and Cisco RFGW-10. You must configure N+1 DEPI redundancy on the M-CMTS router before configuring it on the Cisco RFGW-10.

The working tunnel and the protect tunnel are configured using the same **depi-tunnel** command. The protect tunnel inherits L2TP class and DEPI class parameters from the working tunnel. When you configure the protect tunnel and specify the destination IP address for the protect tunnel, the protect tunnel inherits the QAM channel parameters specified for the working tunnel.

Before You Begin

- You must configure N+1 line card redundancy for the Cisco uBR-MC3GX60V line card before configuring N+1 DEPI redundancy.
- The tunnel names for the working and protect tunnels must be distinct and the protect tunnel must be associated with the corresponding working tunnel.
- The working tunnel must be configured on the M-CMTS router before configuring the protect tunnel.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**depi-tunnel** *protect-depi-tunnel-name* **Example:** `Router(config)# depi-tunnel protect1`	Specifies a protect tunnel name and enters DEPI tunnel configuration mode.

	Command or Action	Purpose
Step 4	**dest-ip** *dest-ip-address* **Example:** `Router(config-depi-tunnel)# dest-ip 192.0.2.103`	Specifies the destination IP address of the termination point for the protect tunnel. **Note** When configuring on the M-CMTS router, destination IP address is the IP address of the EQAM. When configuring on the EQAM, this is the IP address of the M-CMTS router.
Step 5	**exit** **Example:** `Router(config-depi-tunnel)# exit`	Exits the DEPI tunnel configuration mode.
Step 6	**depi-tunnel** *working-depi-tunnel-name* **Example:** `Router(config)# depi-tunnel working1`	Specifies a working tunnel name that is already configured with QAM channel parameters, and enters DEPI tunnel configuration mode.
Step 7	**protect-tunnel** *protect-depi-tunnel-name* **Example:** `Router(config-depi-tunnel)# protect-tunnel protect1`	Associates the protect tunnel to the corresponding working tunnel. **Note** Use the same protect tunnel that you created using the **depi-tunnel** command to associate the protect tunnel to the corresponding working tunnel.
Step 8	**end** **Example:** `Router(config-depi-tunnel)# end`	Exits DEPI tunnel configuration mode and returns to privileged EXEC mode.

Configuring DLM on the M-CMTS Router

This section describes how to configure DLM on the M-CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller modular-cable** {*slot*/*bay*/*port* | *slot*/*subslot*/*controller*}	Specifies the modular cable controller interface for the SPA or the line card.

	Command or Action	Purpose
	Example: `Router(config)# controller modular-cable 1/0/0`	• *slot*—SPA interface processor (SIP) or the line card slot. Slots 1 and 3 are used for SIPs. The valid range is from 5 to 8 for the line card slot. • *bay*—The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). • *port*—Specifies the interface number on the SPA. • *subslot*—Cable interface line card subslot. Valid values are 0 and 1. • *controller*—Controller index for the modular cable. The valid range is from 0 to 2.
Step 4	**rf-channel** *rf-port* **network-delay** {*delay* | **auto**} [**sampling-rate** *rate*] **Example:** `Router(config-controller)# rf-channel rf6 network-delay auto sampling-rate 1`	Configures the network delay for an RF channel. • *rf-port*—RF channel physical port on the SPA or the line card. Valid values for the RF port depend on the configuration of the annex modulation. • *delay*—The Converged Interconnect Network (CIN) delay. The default value is 550 usec. The permitted range is from 0 to 3000 usec. • **auto**—Determines the delay through DLM packets automatically. • **sampling-rate** *rate*—(Optional) Specifies how often the DLM is sent. This option is available only when the network delay value is set as auto. The permitted range is from 1 to 500 sec. The default value is 10 sec.
Step 5	**end** **Example:** `Router(config-controller)# end`	Returns to privileged EXEC mode.

Disabling a DEPI Data Session on the M-CMTS Router

This configuration is optional. This section describes how to disable a DEPI data session on the M-CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller modular-cable** {*slot*/*bay*/*port* | *slot*/*subslot*/*controller*} **Example:** `Router(config)# controller modular-cable 1/0/0`	Specifies the modular cable controller interface for the SPA or the line card. • *slot*—SPA interface processor (SIP) or the line card slot. Slots 1 and 3 are used for SIPs. The valid range is from 5 to 8 for the line card slot. • *bay*—The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay). • *port*—Specifies the interface number on the SPA. • *subslot*—Cable interface line card subslot. Valid values are 0 and 1. • *controller*—Controller index for the modular cable. The valid range is from 0 to 2.
Step 4	**no rf-channel** *rf-channel* **depi-tunnel** *depi-tunnel-name* [**tsid** *id*] **Example:** `Router(config-controller)# rf-channel 0 depi-tunnel SPA0 tsid 100`	Removes the specified DEPI data session under the modular controller. • *rf-channel*—RF channel physical port on the SPA or the line card. • *depi-tunnel-name*—Name of the DEPI tunnel. • **tsid** *id*—(Optional) Specifies the TSID value on the QAM subinterface. The TSID is used to associate the logical RF channel of the SPA or the line card to a physical QAM on Cisco RFGW-10.
Step 5	**end** **Example:** `Router(config-controller)# end`	Returns to Privileged EXEC mode.

Configuration Examples for M-CMTS DEPI Control Plane

This section provides the following configuration examples:

Example: DEPI Control Plane Configuration on the M-CMTS Router

The following example shows how to configure DEPI control plane on the M-CMTS:

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

```
l2tp-class rf6
!
depi-class rf6
mode mpt
!
depi-tunnel rf6
tos 128
dest-ip 192.0.2.103
l2tp-class rf6
depi-class rf6
!
controller Modular-Cable 1/0/0
ip-address 192.0.2.155
modular-host subslot 6/0
rf-channel 6 cable downstream channel-id 7
rf-channel 6 frequency 717000000 annex B modulation 64qam interleave 64
rf-channel 6 depi-tunnel rf6 tsid 6
rf-channel 6 rf-power 46
rf-channel 6 network-delay auto sampling-rate 1
no rf-channel 6 rf-shutdown
.
.
.
```

Example: DEPI Control Plane Configuration on Cisco RFGW-10

The following example shows how to configure DEPI control plane on Cisco RFGW-10:

```
Router# show running-config
.
.
.
l2tp-class rf6
!
depi-class rf6
!
depi-tunnel rf6
dest-ip 192.0.2.155
l2tp-class rf6
depi-class rf6
!
.
.
.
interface Qam6/4
no ip address
!
interface Qam6/4.1
cable mode depi remote learn
cable downstream tsid 6
depi depi-tunnel rf6
snmp trap link-status
!
```

Example: N+1 DEPI Redundancy Configuration on the M-CMTS Router

The following example shows how to configure N+1 DEPI redundancy on the Cisco CMTS router:

```
Router# show running-config
.
.
.
l2tp-class rf6
!
depi-class rf6
mode mpt
!
```

```
depi-tunnel rf6
tos 128
dest-ip 192.0.2.103
l2tp-class rf6
depi-class rf6
protect-tunnel test1_protect
!
depi-tunnel test1_protect
 dest-ip 24.30.14.103
controller Modular-Cable 8/0/0
ip-address 192.0.2.155
modular-host subslot 6/0
rf-channel 6 cable downstream channel-id 7
rf-channel 6 frequency 717000000 annex B modulation 64qam interleave 64
rf-channel 6 depi-tunnel rf6 tsid 6
rf-channel 6 rf-power 46
rf-channel 6 network-delay auto sampling-rate 1
no rf-channel 6 rf-shutdown
.
.
.
```

Example: GigabitEthernet Interface Configuration on the M-CMTS Router

The following example shows the GigabitEthernet configuration on the M-CMTS:

```
Router# show running-config interface gigabitEthernet 1/0/0
.
.
.
interface GigabitEthernet1/0/0
ip address 192.0.2.155 255.255.255.0
negotiation auto
.
.
.
```

Example: GigabitEthernet Interface Configuration on Cisco RFGW-10

The following example shows the GigabitEthernet configuration on RFGW-10:

```
Router# show running-config interface gigabitEthernet 6/13
.
.
.
interface GigabitEthernet6/13
no switchport
ip address 192.0.2.103 255.255.255.0
.
.
.
```

Verifying M-CMTS DEPI Control Plane

This section explains how to verify DEPI control plane configuration on the M-CMTS router, and it contains the following topics:

Verifying DEPI Tunnel Information

To verify a DEPI tunnel information, use the **show depi tunnel** command in privileged EXEC mode.

Note This command works on both the M-CMTS router and the Cisco RFGW-10.

The following is a sample output of the **show depi tunnel** command for all the active control connections:

```
Router# show depi tunnel
LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                             Count VPDN Group
1834727012 3849925733 RFGW-10       est    192.0.2.155       1     rf6
```

The following is a sample output of the **show depi tunnel** command for a specific active control connection identified using the depi-tunnel-name:

```
Router# show depi tunnel 1834727012 verbose
Tunnel id 1834727012 is up, remote id is 3849925733, 1 active sessions
  Locally initiated tunnel
  Tunnel state is established, time since change 04:10:38
  Remote tunnel name is RFGW-10
    Internet Address 192.0.2.155, port 0
  Local tunnel name is myankows_ubr10k
    Internet Address 192.0.2.103, port 0
  L2TP class for tunnel is rf6
  Counters, taking last clear into account:
    0 packets sent, 0 received
    0 bytes sent, 0 received
    Last clearing of counters never
  Counters, ignoring last clear:
    0 packets sent, 0 received
    0 bytes sent, 0 received
  Control Ns 255, Nr 254
  Local RWS 1024 (default), Remote RWS 8192
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 256
    Slow Start threshold, Ssthresh 8192
    Mode of operation is Slow Start
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 2
  Total resends 0, ZLB ACKs sent 252
  Total peer authentication failures 0
  Current no session pak queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0 0
  Control message authentication is disabled
```

Note The counters in the **show depi tunnel verbose** command output are not supported.

The following is a sample output of the **show depi tunnel** command that shows DEPI tunnel endpoints in Cisco IOS Release 12.2(33)SCE and later releases. The **endpoints** keyword is supported only on the M-CMTS router.

```
Router# show depi tunnel endpoints
DEPI Tunnel               Modular Controller   State  Remote Address Sessn
                                                                     Count
depi_working_tunnel_8_0_4 Mod8/0/2             est    1.30.84.100     24
depi_protect_tunnel_5_1_0 Mod8/0/0:5/1/0       est    1.30.50.100     24
depi_protect_tunnel_5_1_4 Mod8/0/2:5/1/2       est    1.30.54.100     24
depi_working_tunnel_8_0_0 Mod8/0/0             est    1.30.3.100      24
```

Verifying DEPI Session Information

To verify a DEPI session, use the **show depi session** command in privileged EXEC mode.

Note This command works on both the M-CMTS router and the Cisco RFGW-10.

The following is a sample output of the **show depi session** command for all the established DEPI data sessions:

```
Router# show depi session
LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
1252018468 1252055513 1834727012 6,                   est    04:06:10 1
```

The following is a sample output of the **show depi session** command for a specific established DEPI data session identified using the *session-id*:

```
Router# show depi session 1252018468 verbose
Session id 1252018468 is up, tunnel id 1834727012
  Remote session id is 1252055513, remote tunnel id 3849925733
  Locally initiated session
Qam Channel Parameters
  Group Tsid is 0
  Frequency is 717000000
  Modulation is 64qam
  Annex is B
  Interleaver Depth I=32 J=4
  Power is 0
  Qam channel status is 0
  Unique ID is 1
Call serial number is 326100007
Remote tunnel name is RFGW-10
  Internet address is 192.0.2.155
Local tunnel name is myankows_ubr10k
  Internet address is 192.0.2.103
IP protocol 115
  Session is L2TP signaled
  Session state is established, time since change 04:06:24
    0 Packets sent, 0 received
    0 Bytes sent, 0 received
  Last clearing of counters never
  Counters, ignoring last clear:
    0 Packets sent, 0 received
    0 Bytes sent, 0 received
    Receive packets dropped:
      out-of-order:             0
      total:                    0
    Send packets dropped:
      exceeded session MTU:     0
      total:                    0
  DF bit on, ToS reflect enabled, ToS value 0, TTL value 255
  UDP checksums are disabled
  Session PMTU enabled, path MTU is 1492 bytes
  No session cookie information available
  FS cached header information:
    encap size = 28 bytes
    45000014 00004000 FF73706F 01030467
    0103049B 4AA0D9D9 00000000
  Sequencing is on
    Ns 0, Nr 0, 0 out of order packets received
    Packets switched/dropped by secondary path: Tx 0, Rx 0
  Conditional debugging is disabled
```

Beginning with Cisco IOS Release 12.2(33)SCE, you can verify DEPI EQAM statistics (this feature is enabled by default), using the **show depi session** command with the **verbose** keyword as shown in the following example:

```
Router# show depi session 1252018468 verbose
Session id 1252018468 is up, tunnel id 1834727012
  Remote session id is 1252055513, remote tunnel id 3849925733
  Locally initiated session
Qam Channel Parameters
  Group Tsid is 0
  Frequency is 717000000
  Modulation is 64qam
  Annex is B
  Interleaver Depth I=32 J=4
  Power is 0
  Qam channel status is 0
  Unique ID is 1
.
.
.
Sequencing is on
    Ns 0, Nr 0, 0 out of order packets received
    Packets switched/dropped by secondary path: Tx 0, Rx 0
.
.
.
Peer Session Details
Peer Session ID : 1073808091
Peer Qam ID : Qam3/12.2
Peer Qam State : ACTIVE
Peer Qam Type : Secondary
Peer Qam Statistics
Total Pkts : 35177
Total Octets : 6613276
Total Discards : 0
Total Errors : 0
Total In Pkt Rate : 0
Bad Sequence Num : 0
Total In DLM Pkts : 0
Conditional debugging is disabled
```

Note The counters in the **show depi session verbose** command output are not supported.

The following is a sample output of the **show depi session** command for all the configured DEPI data sessions:

```
Router# show depi session configured
Session Name           State    Reason                      Time
Modular-Cable1/0/0:0   IDLE     Power mismatch              Jun 10 09:59:07
```

The following is a sample output of the **show depi session** command that shows DEPI session endpoints in Cisco IOS Release 12.2(33)SCE and later releases. The **endpoints** keyword is supported only on the M-CMTS router.

```
Router# show depi session endpoints
DEPI Tunnel               RF Channel             EQAM rf-port Tsid  State  Type
depi_working_tunnel_8_0_0 Mod8/0/0:0             Qam3/7.1     371   est    P
depi_protect_tunnel_5_1_0 Mod8/0/0:5/1/0:0       Qam3/7.1     371   est    S
non_cisco_eqam_tunnel     Mod8/0/0:6             -            11012 est    P
```

Verifying DLM Configuration Information

To verify the DLM configuration information, use the **show interface modular-cable dlm** command in privileged EXEC mode.

The following example shows sample output of the **show interface modular-cable** *slot/bay/port:interface_number* **dlm** command:

```
Router# show interface modular-cable 1/0/0:6 dlm
DEPI Latency Measurements for Modular-Cable1/0/0:6
Current CIN Delay: 146 usecs
Current DLM: 4566
Average DLM (last 10): 1514
Max DLM: 5115
Min DLM: 913
Ingress DLM
#           SysUpTime           Delay (Ticks)
x-----------x-------------------x------------
0           831149              949
1           831159              1168
2           831170              4566
3           831076              1005
4           831087              983
5           831097              1185
6           831108              1139
7           831118              1144
8           831128              2013
9           831139              996
```

Note The M-CMTS sends either ingress or egress DLM requests based on the EQAM capabilities that EQAM reports during DEPI data session establishment.

Additional References

The following sections provide references related to the M-CMTS DEPI Control Plane feature.

Related Documents

Related Topic	Document Title
Cisco Wideband SPA	*Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide* http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ubr10012/b_10k_sip_spa_scg.html
Cisco uBR-MC3GX60V	*Configuring the Cisco uBR-MC3GX60V Cable Interface Line Card* http://www.cisco.com/en/US/products/hw/cable/ps2209/products_installation_and_configuration_guides_list.html

Related Topic	Document Title
Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards and RFCs

Standard	Title
CM-SP-DEPI-I08-100611	Data-Over-Cable Service Interface Specification, Modular Headend Architecture, Downstream External PHY Interface Specification
RFC 3931	Layer Two Tunneling Protocol - Version 3 (L2TPv3)

MIBs

MIB	MIBs Link
• DOCS-IF-M-CMTS-MIB • DOCS-DRF-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for M-CMTS DEPI Control Plane

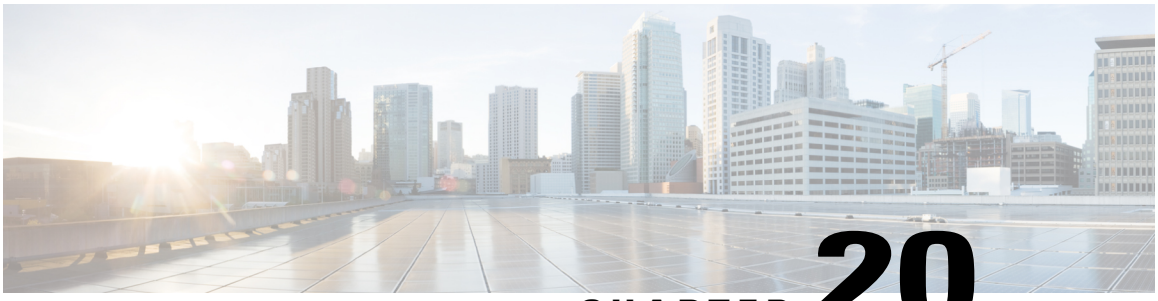
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 43: Feature Information for M-CMTS DEPI Control Plane

Feature Name	Releases	Feature Information
M-CMTS DEPI Control Plane	12.2(33)SCC	This feature was introduced in Cisco IOS Release 12.2(33)SCC. The following commands were introduced or modified: • **depi-class** • **depi-tunnel** • **dest-ip** • **rf-channel depi-tunnel** • **rf-channel rf-power** • **rf-channel rf-shutdown** • **show depi** • **show depi session** • **show depi tunnel**
Ingress DLM	12.2(33)SCC	This feature was introduced in Cisco IOS Release 12.2(33)SCC. The following commands were introduced or modified: • **show interface Modular-Cable dlm** • **rf-channel network-delay**

Feature Name	Releases	Feature Information
N+1 DEPI Redundancy	12.2(33)SCE	Cisco IOS Release 12.2(33)SCE introduces support for the N+1 redundancy for DEPI control plane feature to protect against the Cisco uBR-MC3GX60V line card failure or switchover. The following commands were introduced or modified: • **protect-tunnel** • **show depi session** • **show depi tunnel**
DEPI EQAM Statistics	12.2(33)SCE	The DEPI EQAM statistics feature enables the EQAM to send RF channel statistics to the M-CMTS router. The following command was introduced: • **depi eqam-stats**
DEPI CIN Failover	12.2(33)SCF4	The DEPI CPU threshold values can be configured. The following command was modified: **depi cin-failover cpu-threshold**



CHAPTER 20

Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

First Published: November 16, 2009

Revised Date: May 27, 2013

In Cisco IOS Release 12.2(33)SCC and later releases, support for the restricted load balancing group (RLBG)/general load balancing group (GLBG) is based on DOCSIS 2.0 and 3.0 specifications. Narrowband (NB) dynamic bandwidth sharing (DBS) with dynamic load balancing (DLB) is also supported in Cisco IOS Release 12.2(33)SCC and later releases, and uses RF channel instead of the interface for load balancing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

The Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing feature has the following prerequisites:

- A RLBG and a DOCSIS 2.0 GLBG should have a load balancing group (LBG) ID.
- A LBG should have a default policy ID.
- During registration, a cable modem (CM) that has been assigned to a LBG must also be assigned a policy ID and priority, through Simple Network Management Protocol (SNMP), the CM configuration file, or Cisco Cable Modem Termination System (CMTS) configuration.
- The CM must send service type identifier (STID), service class name, and DOCSIS version and capability type/length/value (TLV) settings to the Cisco CMTS for registration if the fields are used by general tagging.

The table below shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 44: RLBG/GLBG and NB DBS with Downstream DLB Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Card
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2[32] Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20U/H **Note** Starting with Cisco IOS Release 12.2(33)SCH, Cisco uBR10-MC5X20U/H line card is not supported. Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [33]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [34]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

32 PRE = Processor Routing Engine

33 The Cisco uBR3GX60V cable interface line card is compatible only with PRE4.

34 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

The RLBG/GLBG Support and NB DBS Interact with DLB Support feature has the following restrictions:

- Either Cisco load balancing (LB) or DOCSIS LB can be enabled for a MAC domain, but not both.
- A maximum of 256 DOCSIS policies and 256 rules per chassis are supported.
- The **init-tech-ovr** command does not support cross-line card (LC) configuration, as Cisco CMTS always use Dynamic Channel Change (DCC) initialization technique 0 for cross-LC DCC.
- For the restriction about target upstream channel attribute masks, see the "Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers" chapter in the *Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* guide, at the following link:

  http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_load-bal_dcc.html#wp1176797
- We recommend all LBGs that share channels must use the same LB method.
- If a channel is a part of a DOCSIS LBG, use channel selection for CM steering.

The RLBG/GLBG Support and NB DBS Interact with DLB Support feature have the following cross functional restrictions:

- CMs operating in the multiple transmit channel (MTC) mode do not register for a RLBG assignment, even if their configuration file contains relevant TLVs, such as STID and LBG ID. However, CMs operating in the multiple receive channel (MRC) can register for a RLBG assignment.
- A modular cable (MC) interface in DBS mode can join LB operations, using either the modems or service-flows method. However, using the utilization method, if the MC interface is in the DBS mode and sharing the QAM channel with any other wideband (WB) interface that is not using the DBS mode, the LB state of this interface goes down. The MC interface can join LB operations if the interface is not in the DBS mode, or if the interface is in DBS mode and all the WB interfaces sharing the QAM channel are using the DBS mode.
- The Cisco CMTS does not support an MC interface using DBS and sharing the same QAM channel with any other WB interface that is not using DBS. Therefore, the Cisco CMTS does not let the MC interface join a utilization-based LBG. In such cases, the MC interface is in a down status in the utilization-based LBG.

Note The Integrated Cable (IC) interface in DBS mode has the same restrictions as the MC interface.

- The Cisco CMTS can parse a specific TLV encoded in CM configuration file, and prohibit any DCC operation on the CMs.
- DOCSIS MAC domain downstream service group (MD-DS-SG) channels in MDD messages are incorrect when a combination of channels from multiple line card types are placed in the same fiber node. The Cisco uBR-MC20X20V line card MAC domains should only include SPA channels, but if channels from two or more Cisco uBR-MC20X20V line cards are placed in the same fiber node, the MD-DS-SG from one card will include channels from the other line card too.

In a complex fiber node setup, with channels from more than one line card, or downstream channels of one MAC domain in more than one fiber node, some modems may not come w-online (wideband online). If a MAC domain has more than one MD-DS-SG, the MDD will contain more than one MD-DS-SG and cause the modem to perform downstream ambiguity resolution. When the modem analyzes the downstream channels from the other line card, it will not see MDD packets and disqualify the channel and the MD-DS-SG. The modem then sends a requested MD-DS-SG of 0 to the CMTS implying it will not participate in a bonding group.

Use the **show cable mac-domain downstream-service-group** command to see the channels in the same MD-DS-SG.

Use the **debug cable mdd** and **debug cable interface** *mac-domain* on the line card to see that MDDs contain MD-DS-SG with channels from multiple line cards.

The RLBG/GLBG Support and NB DBS Interact with the DLB Support feature have the following scaling limitations:

- The total number of RLBGs and DOCSIS 2.0 GLBGs cannot exceed 256.
- The total number of tags in a Cisco CMTS cannot exceed 256.
- The total number of DOCSIS 3.0 GLBGs is bounded by free memory.
- A CM reset occurs if a CM moves from one cable interface to another because DCC init-tech 0 resets a CM during a LB move. A CM also resets if the two cable interfaces have been configured with a mismatched **cable ip-init** command.

Information About Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

The Cisco implementation on LB is based on the interface and channel on which CMs register, imposing a restriction that a particular DOCSIS channel, upstream (US) or downstream (DS), can only be part of one LBG.

The DOCSIS 2.0 “Autonomous Load Balancing” specification is CM-centric, allowing a channel (US or DS) to be part of multiple RLBGs. Therefore, with the DOCSIS 2.0 specifications, you can decide on which channel the CM can be load balanced.

To configure the Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing feature, you should understand the following concepts:

Service-Based Load Balancing

Using the DOCSIS 3.0 modem-based load balancing specifications, you can manage the LB activity on a per-modem basis as follows:

1. Modem to RLBG association through STID
2. Modem to RLBG association through LBG ID
3. Per-modem LB policy assignment
4. Per-modem LB priority assignment
5. Per-modem channel restriction

Implementing the DOCSIS 3.0 modem-based LB specifications enables the Cisco CMTS to provide an advanced service-based LB. The service-based LB can be used to alleviate the burden for the modem-based provisioning and provide the operator an ability to selectively control LB activity based on modem service type. For example, for LB purposes modems can be classified based on:

- Device type
- DOCSIS version
- Service class

The results of the classification can then be used to selectively control the modem LB activity by mapping the modem to the following settings:

- LBG
- Policy

With the service-based LB enabled, existing service-based cable modem segregation features and channel restriction become special cases and can be handled within the same LB framework. However, the device type-based classification is not available in Cisco IOS Release 12.2(33)SCC.

Functionality

The Cisco CMTS functions in the following ways for general tagging and service-based LB:

- The Cisco CMTS can classify some modems with user-defined modem classifiers using the STID, service class name, DOCSIS version and capability TLVs and MAC Organization Unique Identifier (OUI).
- Each modem classifier has a unique tag. The Cisco CMTS allows each modem to carry one tag. When multiple tags match one cable modem, the tag that has the least index gets applied on the cable modems.
- The Cisco CMTS classifies a CM and assigns a tag, and if a RLBG with that tag is configured, the CM gets assigned to that RLBG.
- The Cisco CMTS can match multiple tags to a RLBG and a DOCSIS policy.
- On the Cisco CMTS, a user can configure whether the general tagging overrides the RLBG or DOCSIS policy assignment using TLVs in the CM configuration file and SNMP when a conflict occurs.
- When doing autonomous LB, the Cisco CMTS ensures that the target channels are available to a specific CM with regard to admission control, the SF attribute masks, and CM attribute masks.
- The user can configure the number of times that a DCC fails a CM before the CM is removed from dynamic LB on the Cisco CMTS.
- The user can configure DCC initialization techniques or whether to use Upstream Channel Change (UCC) for a LBG or for a particular source and target pair on the Cisco CMTS. However, DCC is not issued to cable modems provisioned in DOCSIS 1.0 mode. By default, the UCC for a LBG is not configured and therefore, all channel changes are done through DCC.
- The Cisco CMTS supports LB on at least one logical channel on a physical US channel that has multiple logical US channels.
- As per the DOCSIS 3.0 specifications, a lower load balancing priority indicates a higher likelihood that a CM will be moved due to load balancing operations.

- You can create a policy to set the lower bandwidth for CMs. the LBG can only move cable modems with throughput that is above the threshold.

Compatibility

Both downstream and upstream autonomous load balancing is supported for single channel cable modems on the Cisco uBR10-MC5X20U/H, Cisco UBR-MC20X20V, Cisco uBR-MC88V, Cisco uBR-MC3GX60V line cards, and wideband SPA.

Note The Cisco uBR-MC88V cable interface line card is supported only in Cisco IOS Release 12.2(33)SCD and later releases.

RLBG/GLBG Assignment

Cable modems operating in the MTC mode do not participate in registration for RLBG assignment, even if their configuration file contains relevant TLVs such as STID and LBG ID.

The user can configure one or more service type IDs for each RLBG. The user can also configure the Cisco CMTS, using CLI or SNMP, to restrict a particular cable modem to a certain STID and RLBG ID. However, if such a configuration is made, both the STID and RLBG ID in the configuration file are ignored by the Cisco CMTS.

When the STID is configured by CLI or SNMP or the STID is present in the cable modem configuration file, the Cisco CMTS selects an upstream and downstream channel, which offers the signaled service type, from a RLBG, if such channels exist. However, if an upstream and downstream channel do not exist that provide the signaled service type the Cisco CMTS assigns an upstream and downstream channel that does not offer the signaled service type.

When the LBG ID is configured by CLI or SNMP or the LBG ID is present in the cable modem configuration file, the Cisco CMTS examines the available choices for upstream and downstream channels and, if they include a channel pair associated with the signaled LBG, the Cisco CMTS assigns the cable modem to the signaled LBG. If these conditions are not met, the Cisco CMTS disregards the LBG ID.

If there are multiple upstream and downstream channels available that meet the requirements of the STID, if present, and the LBG ID, if present, the Cisco CMTS selects an upstream and/or downstream channel that meet the cable modem required and forbidden attribute masks requested in the configuration file. If upstream and downstream channels are not available that meet these criteria, the Cisco CMTS can disregard the cable modem attribute masks and select an alternative upstream and/or downstream channel.

In determining a target channel pair for a cable modem during registration time, the Cisco CMTS tries to find the target channel pair that can actually reach the cable modem by checking the current channel pair, the MD-DS-SG-ID (Media Access Control Domain Downstream Service Group Identifier) of cable modem (CM-DS-SG-ID) and the MD-US-SG-ID (Media Access Control Domain Upstream Service Group Identifier) of cable modem (CM-US-SG-ID), if present, and fiber node (FN) configurations. If the target channel pair is available to the cable modem and is different from the current channel pair, the Cisco CMTS is required to move the CM by means of DCC technique 0 or downstream frequency override (DFO).

In Cisco IOS Release 12.2(33)SCE and earlier releases, when the Cisco CMTS identifies multiple candidate RLBGs for a CM, but cannot determine which fiber node configuration the cable modem is actually wired to, or cannot determine if the wired RLBG is unusable (when interfaces in the load balance group are disabled or in an administratively down state), the Cisco CMTS assigns the cable modem to the RLBG with the lowest

group index. This assignment causes the Cisco CMTS to attempt to move the cable modem to interfaces it is not physically connected to, resulting in service outages for the CM.

However, in Cisco IOS Release 12.2(33)SCE1 and later releases, the Cisco CMTS enforces fiber node checking during RLBG assignment.

The Cisco CMTS follows the following RLBG assignment rules:

- If there is no fiber node configuration, there is no change in the candidate RLBG list. However, if the fiber node is configured, the fiber node must be configured correctly to reflect the real fiber node connection.
- If the cable modem is inside a fiber node, only those RLBGs that are inside that fiber node are selected.
- If the cable modem is not inside any fiber node, that is, the fiber node configuration does not cover all the channels, only those RLBGs that are not inside any fiber node are selected.
- If an RLBG spans across multiple fiber nodes, it is not considered to be inside any fiber node.
- If no candidate RLBG is found, cable modems are assigned to the GLBG, if the GLBG exists.

Channel Assignment

For cable modems operating in MRC mode, the registration request message can have multiple TLVs to influence the selection of upstream and downstream channels that the Cisco CMTS assigns. To avoid conflicts between the multiple TLVs, the Cisco CMTS follows the precedence order defined below:

1. TLV 56—Channel Assignment
2. TLV 43.11—Service Type Identifier
3. TLV 43.3—Load Balancing Group ID
4. TLVs 24/25.31-33—Service Flow Attribute Masks
5. TLV 43.9—CM Attribute Masks

The Cisco CMTS must follow this TLV precedence order for cable modems not operating in MRC mode:

1. TLV 43.11—Service Type Identifier
2. TLV 43.3—Load Balancing Group ID
3. TLV 43.9—CM Attribute Masks
4. TLVs 24/25.31-33—Service Flow Attribute Masks

Note Starting with Cisco IOS Release 12.2(33)SCF, cable modems in MTC mode are assigned to load balancing groups.

Note When a target for the new receive channel configuration (RCC) is selected, ensure that the service level for cable modems is not decreased. Target total RCCs must not be less than the source total RCCs so that cable modems can keep their service level unchanged. This may cause some unbalanced results when high capacity cable modems come online, later releases. This limitation will be addressed in a later releases release.

The Cisco CMTS also considers the DOCSIS 3.0 cable modem capabilities defined in the registration request message and assigns the maximum number of channels that the CM requests.

The tables below define the load balancing matrix for RLBG and GLBG assignment:

Table 45: RLBG Assignment for DOCSIS Cable Modems

Operational Mode	MAC Version				
	DOCSIS 3.0 CM	**DOCSIS 2.x CM**	**DOCSIS 2.0 CM**	**DOCSIS 1.1 CM**	**DOCSIS 1.0 CM**
Non-MRC mode (online)	Assigned	Assigned	Assigned	Assigned	Assigned
MRC mode only (w-online)	Assigned	Assigned	Assigned	NA	NA
MRC/MTC mode (UB-online)	Not assigned	NA	NA	NA	NA
	In Cisco IOS Release 12.2(33)SCF, DOCSIS 3.0 cable modems are assigned to the DOCSIS 3.0 RLBG	NA	NA	NA	NA

Table 46: GLBG Assignment for DOCSIS Cable Modems

Operational Mode	MAC Version				
	DOCSIS 3.0 CM	**DOCSIS 2.x CM**	**DOCSIS 2.0 CM**	**DOCSIS 1.1 CM**	**DOCSIS 1.0 CM**
Non-MRC mode (online)	Assigned to the DOCSIS 2.0 GLBG without MD-DS-SG-ID/MD-US-SG-ID				
	Assigned to the DOCSIS 3.0 GLBG with MD-DS-SG-ID/MD-US-SG-ID		NA	NA	NA
MRC mode only (w-online)	Assigned to the DOCSIS 2.0 GLBG without MD-DS-SG-ID/MD-US-SG-ID				
	Assigned to the DOCSIS 3.0 GLBG with MD-DS-SG-ID/MD-US-SG-ID		NA	NA	NA
MRC/MTC mode (UB-online)	Not assigned	NA	NA	NA	NA
	In Cisco IOS Release 12.2(33)SCF, DOCSIS 3.0 cable modems are assigned to the DOCSIS 3.0 RLBG	NA	NA	NA	NA

The table below displays the change in behavior in channel assignment between Cisco IOS Release 12.2(33)SCE and earlier releases, and Cisco IOS Release 12.2(33)SCF:

Table 47: Comparison of Load Balancing Move of cable modems with LBG Assignment

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Cisco IOS Release 12.2(33)SCE and earlier	Cisco IOS Release 12.2(33)SCF
DOCSIS 3.0 CM in MTC mode	NA	WB/UB	DS/US	NA	• If RLBG is not found in the FN to get cable modems online, is not assigned an RLBG ID. • CM is assigned an LBG ID if any RLBG is available in the FN. • cable modems inside an RLBG or GLBG are added to the modem list. • cable modems outside an RLBG stay outside, are not added to the modem list
DOCSIS 3.0/DOCSIS 2.x cable modems in MRC-only mode	NA	WB/UB	DS	• If RLBG is not found in the FN to get cable modems online, is not assigned an RLBG ID. • CM is assigned an LBG ID if any RLBG is available in the FN. • Primary channel of the CM and upstream inside RLBG or GLBG is added to modem list. • cable modems outside an RLBG are added to the modem list after moving the primary channel and upstream channels inside the RLBG.	Same as in Cisco IOS Release 12.2(33)SCE.

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Cisco IOS Release 12.2(33)SCE and earlier	Cisco IOS Release 12.2(33)SCF
DOCSIS 3.0 cable modems in MRC-only mode	DOCSIS 2.0 dynamic modem count-based LB (MCBLB), dynamic utilization	NB	US	Same as above.	Same as in Cisco IOS Release 12.2(33)SCE.
DOCSIS 2.0 /DOCSIS 1.1 cable modems in NB mode	DOCSIS 2.0 dynamic MCBLB, dynamic utilization	NB	DS/US	Same as above.	Same as in Cisco IOS Release 12.2(33)SCE.

Table 48: Comparison of Load Balancing Move of cable modems with LBG Assignment

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Movement
DOCSIS 3.0 CM in MTC mode	NA	WB/UB	DS/US	• If RLBG is not found in the FN to get cable modems online, is not assigned an RLBG ID. • CM is assigned an LBG ID if any RLBG is available in the FN. • Cable modems inside an RLBG or GLBG are added to the modem list. • Cable modems outside an RLBG stay outside, are not added to the modem list

Modem Mode	Load Balancing Method	Load Balancing Counters	Channels	Movement
DOCSIS 3.0/DOCSIS 2.x cable modems in MRC-only mode	NA	WB/UB	DS	• If RLBG is not found in the FN to get cable modems online, is not assigned an RLBG ID. • Cable modem is assigned an LBG ID if any RLBG is available in the FN. • Primary channel of the cable modem and upstream inside RLBG or GLBGis added to modem list . • Cable modems outside an RLBG are added to the modem list after moving the primary channel and upstream channels inside the RLBG
DOCSIS 3.0 cable modems in MRC-only mode	DOCSIS 2.0 dynamic modem count-based LB (MCBLB), dynamic utilization	NB	US	Same as above.
DOCSIS 2.0 /DOCSIS 1.1 cable modems in NB mode	DOCSIS 2.0 dynamic MCBLB, dynamic utilization	NB	DS/US	Same as above.

The tables below give a snapshot view of the load balancing methods and the operations used to "move" bonded and non-bonded CMs.

Table 49: Load Balancing Method to Move Bonded and Non-bonded cable modems

Modem Mode	Dynamic Service Charge (Initialization Technique)	
	Within MAC Domain	**Across MAC Domains**
DOCSIS 3.0 cable modems in MTC mode	NA	DCC initialization technique 0
DOCSIS 3.0/DOCSIS 2.x cable modems in MRC-only mode	DCC initialization technique 0 **Note** CM with primary DS outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC initialization technique 0

Modem Mode	Dynamic Service Charge (Initialization Technique)	
DOCSIS 3.0 cable modems in MRC-only mode	DCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC initialization technique 0
DOCSIS 2.x cable modems in MRC-only mode	DCC/UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC initialization technique 0
DOCSIS 2.0 /DOCSIS 1.1 cable modems in NB mode	DCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	DCC initialization technique 0
	UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	UCC
DOCSIS 1.0 in NB mode	Force reinitialize CM **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	Force reinitialize CM
	UCC **Note** CM outside RLBG moves inside RLBG with DOCSIS 2.0 LB.	UCC

Table 50: Using DCC/DBC to Load Balance Bonded and Non-bonded Cable Modems

Channel	CM in MRC, non-MTC Mode	DOCSIS 1.1/DOCSIS 2.0 cable modems with Single US/DS	DOCSIS 1.0 cable modems with Single US/DS
Upstream (US)	DCC	DCC	UCC
Downstream (DS)	NA (within the same MAC domain)	DCC (within the same MAC domain).	Force reinitialize CM
	DCC with initialization technique 0 when moving cable modems across MAC domains.	DCC with initialization technique 0 when moving cable modems across MAC domains.	Force reinitialize CM

Error Handling of Channel Assignment

In Cisco IOS Release 12.2(33)SCE and earlier releases, the interface state of the channels is considered when determining load balancing groups (LBG) assignment. Only those channels that are in the "initial", "up", "suspicious", or "testing" states are available for LBG assignment.

However, in Cisco IOS Release 12.2(33)SCF, this restriction is modified. As long as the interface state of the channels is not "administratively down", all channels are available for LBG assignment. For other load balancing operations, such as moving modems using DCC, UCC, or DBC, the interface state of the channels should be in "initial", "up", "suspicious", or "testing" states.

Effective with Cisco IOS Release 12.2(33)SCF1, the following conditions apply when an LBG is disabled:

- cable modems that match all load balancing criteria can be assigned to an LBG.
- cable modem moves for load balancing are disabled, but cable modem moves from outside of the LBG to inside of the LBG are allowed.

Upstream Load Balancing for DOCSIS 3.0 Cable Modems in Single Upstream Mode

The upstream load balancing functionality enables the Cisco CMTS router to effectively handle upstream traffic for wideband and narrowband cable modems that are in single upstream mode. Single upstream mode (Mx1) means that the modems cannot send upstream traffic on multiple upstream channels. In the event of traffic overload on a single upstream channel of a wideband or narrowband cable modem, the Cisco CMTS router automatically moves the cable modem to another upstream channel in the same load balancing group.

Note A cable modem operating in single upstream mode is assigned to a load balancing group based on the primary channel of the modem. A cable modem in single upstream mode can support multiple receive channel (MRC) mode or narrowband mode. However, a cable modem in single upstream mode cannot support multiple transmit channel mode (MTC).

Narrowband LB with DBS

In earlier releases, there was a restriction on an MC interface using dynamic bandwidth sharing to be included in a LBG. Starting with Cisco IOS Release 12.2(33)SCC, a new measurement of link utilization is introduced to overcome this restriction of load balancing on an MC interface using DBS. The modem count and service flow count-based loads in DBS are refined to be consistent with the DBS functionality.

Note The Integrated Cable (IC) interface in DBS mode has the same measurement as the MC interface.

Functionality

The Cisco CMTS can balance the utilization of underlying QAM channels across LBG using the utilization method. There is no restriction for all MC interfaces in the LBG to use DBS.

The Cisco CMTS can balance the modem count or service flow count as follows:

- The guaranteed bandwidth of each MC interface across LBG using the modem count or service flow count method, if all MC interfaces in that LBG are using DBS.
- The guaranteed bandwidth of an MC interface using DBS and the nominal bandwidth of an MC interface that is not using DBS across the LBG using the modem count or service flow count method, even if all MC interfaces in that LBG are not using DBS.

Compatibility

Narrowband LB with DBS is supported on the Cisco 10000 SIP-600 and Cisco uBR-MC88V cable interface line card.

Note The Cisco uBR-MC88V cable interface line card is supported only in Cisco IOS Release 12.2(33)SCD and later releases.

Auto-generate DOCSIS 2.0 GLBG

Cisco CMTS does not automatically implement DOCSIS 2.0 GLBG. DOCSIS 2.0 GLBG is configured manually after a new fiber node - MAC domain (FN-MD) pair is added.

Cisco IOS Release 12.2(33)SCH introduces an enhancement to automatically generate DOCSIS 2.0 GLBG after adding a new FN-MD pair and resolving a new combination of MAC domain, cable modem, and service group (MD-CM-SG). This enhancement is implemented through a new command **cable load-balance d20 GLBG auto-generate**. The command has options to renew and update DOCSIS 2.0 GLBGs for a fiber node configuration.

Independent Upstream/Downstream Throughput Rules

Currently, during upstream or downstream load balancing, to move modems in load balancing operations, Cisco CMTS applies the DOCSIS policy throughput rules to both upstream and downstream throughput to upstream or downstream load balancing operations. In other words, for downstream load balancing, both upstream and downstream sets of rules are applied and similarly for upstream load balancing both set of rules are applied. This prevents movement of modems with low upstream or high downstream throughput and high upstream or low downstream throughput.

Effective with Cisco IOS Release 12.2(33)SCH, upstream or downstream throughput rules are checked independently to corresponding upstream or downstream load balancing operations. During upstream load balancing, only upstream throughput rules are checked, and during downstream load balancing, only downstream throughput rules are checked.

The following important points are implemented for independent upstream/downstream throughput rules:

- If a load balancing operation involves a change only in the downstream channel of a cable modem without any change to the upstream channel, then only the downstream lower boundary rules are checked.
- If a load balancing operation involves a change only in the upstream channel of a cable modem without any change to the downstream channel, then only the upstream lower boundary rules are checked.
- If a load balancing operation involves a change in both the upstream and downstream channels of a cable modem, then the modem rule check must pass all the rules for that (upstream or downstream) load balancing.
- If the load balancing policy configured is **pure-ds-load**, then only the downstream rules are checked.
- If the load balancing policy configured is **us-across-ds** or both **us-across-ds** and **pure-ds-load**, then two types of target interfaces occur as follows:
    - Local interface—where the cable modem shares the upstream with the source. Only downstream load balancing operation occurs.
    - Remote interface—where the the cable modem does not share the upstream with the source. The upstream/downstream load balancing is triggered by upstream load.

If the load balancing policy configured is neither us-across-ds nor pure-ds-load, then the load balancing is done based on Mac domain load.

How to Configure Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

The Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing feature can be configured as follows:

- A user can configure a DOCSIS 2.0 general load balancing group (GLBG) on the Cisco CMTS according to DOCSIS specification. The Cisco CMTS creates a DOCSIS 3.0 GLBG for each Media Access Control Domain Cable Modem Service Group (MD-CM-SG) automatically and checks whether the GLBG contains both upstream and downstream channels.
- A CM that is not provisioned to any RLBG and cannot resolve its MD-CM-SG gets assigned to a DOCSIS 2.0 GLBG. However, if the CM resolves its MD-CM-SG, it gets assigned to a DOCSIS 3.0 GLBG.
- A user can configure RLBGs and any upstream or downstream channel into multiple RLBGs on the Cisco CMTS. The Cisco CMTS checks whether a RLBG contains both upstream and downstream channels. A RLBG can cross multiple MDs.
- A backward compatibility with existing Cisco LB schemes is maintained. The users can switch between the old and new DOCSIS 3.0 compliant LB schemes.

Note When the Cisco IOS system is upgraded from Cisco IOS Release 12.2(33)SCE6 to Cisco IOS Release 12.2(33)SCH2, the docsis-policy configuration of the DOCSIS load balancing groups, is missing in the output of the **show running-config** command. Legacy load balancing groups are not affected by this software upgrade.

Effective with Cisco IOS Release 12.2(33)SCH2, after the software is upgraded from Cisco IOS Release 12.2(33)SCE6 to Cisco IOS Release 12.2(33)SCH2, apply the docsis-policy to the DOCSIS load balancing groups using the **docsis-policy** *policy-id* command again.

The following sections describe how to create and configure DOCSIS load balancing groups to enable DOCSIS load balancing on the Cisco CMTS:

Configuring DOCSIS 3.0 and 2.0 RLBG and DOCSIS 2.0 GLBG

This section describes how to create and configure a DOCSIS load balancing group. There is a separate configuration mode for a DOCSIS load balancing group that is different from the legacy load balancing group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-enable** **Example:** `Router(config)# cable load-balance docsis-enable`	Enables DOCSIS load balancing on the Cisco CMTS.
Step 4	**cable load-balance docsis-group** *docsis-group-id* **Example:** `Router(config)# cable load-balance docsis-group 1`	Creates a DOCSIS load balance group on the Cisco CMTS, with the following parameter: The router enters DOCSIS load balancing group configuration mode.
Step 5	**init-tech-list** *tech-list* [**ucc**] **Example:** `Router(config-lb-group)# init-tech-list 1 ucc`	Sets the DCC initialization techniques that the Cisco CMTS can use to load balance cable modems.
Step 6	**downstream** {**Cable** {*slot/subslot/port* | *slot/port*} | **Integrated-Cable** {*slot/subslot/bay* | *slot/port*} {**rf-channel** *group list*}| **Modular-Cable** {*slot/subslot/bay* | *slot/port*} {**rf-channel** *group list*}} **Example:** `Router(config-lb-group)# downstream integrated-Cable 5/0/0 rf-channel 2`	Sets the downstream RF channels. **Note** The **Integrated-Cable** and **Modular-Cable** parameters are available only on the Cisco uBR10012 universal broadband router.
Step 7	**upstream Cable** {*slot/subslot/port* | *slot/port*} *upstream-list* **Example:** `Router(config-lb-group)# upstream Cable 1/0 2`	Sets upstream channels with the following parameters:

	Command or Action	Purpose
Step 8	**docsis-policy** *policy-id* **Example:** `Router(config-lb-group)# docsis-policy 0`	Assigns a policy to a group with the parameter that becomes the default policy assigned to the CM, if the CM does not choose a different policy.
Step 9	**restricted** **Example:** `Router(config-lb-group)# restricted`	Selects the restricted group type. By default, the general group type is selected.
Step 10	**init-tech-ovr Cable** {*slot/subslot/port* | *slot/port*} *upstream* **Cable** {*slot/subslot/port* } | *slot/port upstream* **init-tech-list** *0-4* [**ucc**] **Example:** `Router(config-lb-group)# init-tech-ovr Cable 8/1/0 0 Cable 8/1/1 1 init-tech-list 1 ucc`	Sets DCC initialization techniques that overrides the physical upstream channel pair. The **init-tech-ovr** command can also be used to determine whether the UCC can be used for modems during dynamic upstream load balancing. The following parameters override the physical upstream channel pair: **Note** The **init-tech-list** keyword accepts an upstream that is not added into the load balancing group. The upstream channel pair is invalid until the upstream is added. When the load balancing group is removed, all upstream channel pairs are also removed.
Step 11	**service-type-id** *string* **Example:** `Router(config-lb-group)# service-type-id commercial`	Adds a service type ID, with the following parameter, that is compared against the cable modem provisioned service type ID, to determine an appropriate restricted load balancing group (RLBG):
Step 12	**tag** *tag name* **Example:** `Router(config-lb-group)# tag t1`	Adds a tag to the RLBG.
Step 13	**interval** <*1-1000*> **Example:** `Router(config-lb-group)# interval 60`	Sets the time interval, the Cisco CMTS waits before checking the load on an interface.

	Command or Action	Purpose
Step 14	**method** {**modems** | **service-flows** | **utilization**} {**us-method** {**modems** | **service-flows** | **utilization**}} **Example:** `Router(config-lb-group)# method modems us-method modems`	Selects the method the Cisco CMTS use to determine the load.
Step 15	**policy** {**pcmm** | **ugs** | **us-across-ds** | **pure-ds-load**} **Example:** `Router(config-lb-group)# policy us-across-ds` `Router(config-lb-group)# policy ugs` `Router(config-lb-group)# policy pure-ds-load`	Selects the modems based on the type of service flow that are balanced.
Step 16	**threshold** {**load** {**minimum** *<1-100>* | *<1-100>*}| **pcmm** *<1-100>* | **stability** *<0-100>* | **ugs** *<1-100>*} **Example:** `Router(config-lb-group)# threshold load minimum 10` `Router(config-lb-group)# threshold pcmm 70` `Router(config-lb-group)# threshold load 10` `Router(config-lb-group)# threshold stability 50` `Router(config-lb-group)# threshold ugs 70`	Selects the percentage of use beyond which load balancing occurs.
Step 17	**exit** **Example:** `Router# exit`	Exits DOCSIS LBG configuration.

Configuring DOCSIS 3.0 GLBG

The following sections describe how to configure a DOCSIS 3.0 GLBG and also how to configure default values of DOCSIS 3.0 certification for the DOCSIS 3.0 general group:

Note Starting with Cisco IOS Release 12.2(33)SCF1, when a Cable interface on the Cisco uBR10-MC5X20U/H line card is shut down, the associated DOCSIS 3.0 GLBGs are removed from the running-configuration. However, if the Cable interface is later releases 'no shut', the configuration of the GLBGs is restored in the running-configuration. This behavior is now consistent with the Cable interfaces on the Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards.

Configuring a DOCSIS 3.0 General Load Balancing Group

This section describes how to configure a DOCSIS 3.0 general load balancing group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance docsis-enable** **Example:** `Router(config)# cable load-balance docsis-enable`	Enables DOCSIS load balancing on the Cisco CMTS.
Step 4	**cable load-balance docsis-group FN** *fn-id* **MD** *cable* {*slot/subslot/port* | *slot/port*} **Example:** `Router(config)# cable load-balance docsis-group FN 1 MD c5/0/0`	Enters the DOCSIS load balancing group configuration mode.
Step 5	**init-tech-list** *tech-list* [**ucc**] **Example:** `Router(config-lb-group)# init-tech-list 1 ucc`	Sets the DCC initialization technique list, with the following parameters.
Step 6	**disable** **Example:** `Router(config-lb-group)# disable`	Disables the load balance group.
Step 7	**docsis-policy** *policy-id* **Example:** `Router(config-lb-group)# docsis-policy 0`	Sets the load balance group policy.
Step 8	**interval** *1-1000* **Example:** `Router(config-lb-group)# interval 10`	Sets the interface polling interval.
Step 9	**method** {**modems** | **service-flows** | **utilization**} {**us-method** {**modems** | **service-flows** | **utilization**}} **Example:** `Router(config-lb-group)# method modems us-method modems`	Sets the load balancing type or method.

	Command or Action	Purpose
Step 10	**policy** {**pcmm** | **ugs** | **us-across-ds** | **pure-ds-load**} **Example:** `Router(config-lb-group)# policy us-across-ds`	Sets load balancing policy.
Step 11	**threshold** {**load** {**minimum** *1-100* | *1-100*} | **pcmm** *1-100* | **stability** *0-100* | **ugs** *1-100*} **Example:** `Router(config-lb-group)# threshold pcmm 70`	Sets the load balancing threshold in percentage.
Step 12	**exit** **Example:** `Router# exit`	Exits the DOCSIS load balancing group configuration mode.

Configuring Default Values of DOCSIS 3.0 Load Balancing Group

This section describes how to configure default values of DOCSIS 3.0 certification for a DOCSIS 3.0 general group on the Cisco CMTS. A DOCSIS 3.0 general group is automatically created for each MD-CM-SG derived from the fiber node (FN) configuration, and the group parameters are set as default values.

Note The configured default values of DOCSIS 3.0 certification are applicable to the new automatically created DOCSIS 3.0 GLBGs and do not affect the existing DOCSIS 3.0 GLBGs. When a DOCSIS 3.0 GLBG is removed and recreated, its group parameters do not change.

Note Starting with Cisco IOS Release 12.2(33)SCH, the default settings for interface polling interval, load balancing method, policy for modems selection, and threshold usage in percent, can be configured for DOCSIS 3.0 general group. For more information, see the Cisco IOS CMTS Cable Command Reference.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable load-balance d30-ggrp-default disable** **Example:** `Router(config)# cable load-balance d30-ggrp-default disable`	Disables the default values of the DOCSIS 3.0 general load balance group (GLBG).
Step 4	**cable load-balance d30-ggrp-default init-tech-list** *tech-list* **Example:** `Router(config)# cable load-balance d30-ggrp-default init-tech-list 1`	Sets the default DOCSIS 3.0 GLBGs DCC and dynamic bonding change (DBC) initialization techniques.
Step 5	**cable load-balance d30-ggrp-default docsis-policy** *0-0xffffffff* **Example:** `Router(config)# cable load-balance d30-ggrp-default docsis-policy 2`	Sets the default DOCSIS 3.0 GLBGs policy ID.
Step 6	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Configuring Cable Modems to RLBG or a Service Type ID

This section shows how to configure a list of cable modems that are statically provisioned at the Cisco CMTS to a RLBG or a service type ID.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable load-balance restrict modem** *index mac-addr* [*mac-mask*] {**docsis-group** *docsis-group-id* | **service-type-id** *string*} **Example:** `Router(config)# cable load-balance restrict modem 1 001a.c30c.7eee FFFF.FFFF.0000 docsis-group 100`	Assigns a modem or a group of modems with a common MAC mask to a load balancing group or a service type ID.
Step 4	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Configuring Rules and Policies

This section shows how to create and configure rules and DOCSIS policies to restrict the movement of modems during load balancing. Rules determine whether a modem can be moved and during which time periods. The time periods are measured in seconds with the start time being an offset from midnight measured in seconds. Rules are created individually and can be combined into policies. The user is able to create DOCSIS policies that consist of one or more rules. When more than one rule is part of a DOCSIS policy, all rules apply. Each group has a default DOCSIS policy.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance rule** *rule-id* **Example:** `Router(config)# cable load-balance rule 1`	Creates a rule to prevent the modem from being moved.
Step 4	**cable load-balance rule** rule-id {**enabled** | **disabled** | {**disable-period dis-start** *0-86400* **dis-period**	Configures the rule. **Note** Static multicast groups should be configured on the appropriate bundle interface as well as on the correct forwarding interfaces to enable this rule. This feature will not be supported on load balancing groups which are derived from fiber node configuration and with multicast encryption.

	Command or Action	Purpose
	<0-86400>} | **disable-throughput-lowerbound ds** | **us** *thrupt in kbps* | **vdoc-enabled}** **Example:** `Router(config)# cable load-balance rule 1 disable-period dis-start 40 dis-period 50`	
Step 5	**cable load-balance docsis-policy** *policy-id* **rule** *rule-id* **Example:** `Router(config)# cable load-balance docsis-policy 2 rule 1`	Associates a particular rule with the DOCSIS policy with the following parameters:
Step 6	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Troubleshooting Tips

Problem When you disable load balancing and enable it for the next day using the **cable load-balance rule** *rule-id* **disable-period dis-start** *start-time* **dis-period** *disable-period* command, the load balancing is enabled at 12.00 am instead of the configured *disable-period*.

Possible Cause Load balancing rule cannot be disabled and enabled on the next day (that is, after 24 hours) using a single load balancing rule.

Solution Configure separate load balancing rules for disabling load balancing and enabling it on the next day. Configure the rule to disable load balancing using the **cable load-balance rule** *rule-id* **disable-period dis-start** *start-time* **dis-period 0** command. Configure the rule to enable load balancing using the **cable load-balance rule** *rule-id* **disable-period dis-start 0 dis-period** *disable-period* command to enable it for the next day.

Configuring Load Balancing Parameter for a Cable Modem Movement Failure

This section describes how to configure the number of times a CM can fail before the CM is removed from the dynamic load balancing group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable load-balance modem max-failures** *0-100* **Example:** `Router(config)# cable load-balance modem max-failures 10`	Configures the number of times a CM can fail before the CM is removed from the dynamic load balancing group.
Step 4	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Creating and Configuring TLV type Tag

Cisco IOS Release 12.2(33)SCH introduces the **tlv** command for TLV type configuration.

The tags for TLV type matching rule are created and configured in this section.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable tag** *1-1000* **Example:** `Router(config)# cable tag 1`	Creates a tag. Enters the cmts-tag configuration mode.
Step 4	**name** *tag name* **Example:** `Router(cmts-tag)# name CSCO`	Specifies the name of the tag.
Step 5	[**exclude**] **service-type-id** *service-type-id* **Example:** `Router(cmts-tag)# service-type-id HSD`	Configures the specified service type ID for the tag.

	Command or Action	Purpose
Step 6	[**exclude**]**service-class** *service-class-name* **Example:** `Router(cmts-tag)# service-class work`	Configures the specified service class name for the tag.
Step 7	[**exclude**] **docsis-version** *docsis version* **Example:** `Router(cmts-tag)# docsis-version docsis20`	Configures the specified DOCSIS version of the cable modem for the tag.
Step 8	**[exclude] oui** *oui of CM* **Example:** `Router(cmts-tag)# oui 00.1a.c3`	Configures the specified OUI of the cable modem for the tag.
Step 9	[**exclude**] **tlv** *type value* **Example:** `Router(cmts-tag)# tlv mrcs 4`	Configures the specified TLV type for the tag.
Step 10	**override** **Example:** `Router(cmts-tag)# override`	Overrides the TLV or SNMP during load balancing an RLBG.
Step 11	**exit** **Example:** `Router(cmts-tag)# exit`	Exits the cmts-tag configuration mode.
Step 12	**cable load-balance docsis-group** *docsis-group-id* **Example:** `Router(config)# cable load-balance docsis-group 1`	Creates a DOCSIS load balancing group on the Cisco CMTS. If the DOCSIS load balancing group is already present, the router enters the specified DOCSIS load balancing group configuration mode.
Step 13	**tag** *tag name* **Example:** `Router(config-lb-group)# tag CSCO`	Adds a tag to the load balancing group.
Step 14	**exit** **Example:** `Router(config-lb-group)# exit`	Exits the DOCSIS load balancing group configuration mode.
Step 15	**cable load-balance docsis-policy** *policy-id* **tag** *tag name* [**override**] **Example:** `Router(config)# cable load-balance docsis-policy 2 tag CSCO`	Creates a DOCSIS policy and associates a new rule or an existing rule with the policy.

	Command or Action	Purpose
Step 16	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Configuration Examples for Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

This section describes a sample configuration example for configuring Restricted/General Load Balancing and narrowband dynamic bandwidth sharing with downstream dynamic load balancing:

Example: Configuring a Tag

The following example shows how you can configure the tag to exclude a DOCSIS version, a MAC address, a service class name or a service type ID:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# exclude ?
  docsis-version   set the match rule for docsis version
  oui              set the match rule for oui
  service-class    set the match rule for service class name
  service-type-id  set the match rule for service type id
Router(cmts-tag)# exclude docsis-version ?
  docsis10  Match docsis 1.0 modems
  docsis11  Match docsis 1.1 modems
  docsis20  Match docsis 2.0 modems
  docsis30  Match docsis 3.0 modems
Router(cmts-tag)# exclude docsis-version docsis10
Router(cmts-tag)# exclude oui ?
  WORD  OUI of the vendor in the format xx.xx.xx or xx:xx:xx
Router(cmts-tag)# exclude oui 00.1a.c3
Router(cmts-tag)# exclude service-class ?
  WORD  Service class name
Router(cmts-tag)# exclude service-class work
Router(cmts-tag)# exclude service-type-id ?
  WORD  Service Type ID
Router(cmts-tag)# exclude service-type-id commercial
```

Example: Disabling Load Balancing

Use the following commands to disable DOCSIS 3.0 GLBG:

```
Router(config)# cable load-balance docsis-group FN 1 MD cable 6/0/0
Router(config-lb-group)# disable
Router(config-lb-group)#
```

Use the following commands to disable DOCSIS 3.0 RLBG:

```
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# disable
Router(config-lb-group)#
```

Verifying Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

This section describes how to use certain show commands to verify the configuration of the Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable load-balance docsis-group** {*docsis-group-id* | **FN** *fn-id* **MD cable** {*slot/subslot/port* | *slot/port*}} [**all** | **load** | **pending** | **statistics** | **target** | **modem-list** | **primary-load**] **Example:** `Router# show cable load-balance docsis-group 1` `Router# show cable load-balance docsis-group fn 1 MD c8/1/4`	Displays real-time configurational, statistical, and operational information of the load balancing operations on the router.
Step 3	**show cable fiber-node** *fiber-node-id* [**spectrum**] **Example:** `Router# show cable fiber-node 3`	Displays information about a fiber node.
Step 4	**show cable load-balance** [**group** *n*] | [**all** | **load** | **pending** | **statistics** | **target** | **fiber-node-validation**] **Example:** `Router# show cable load-balance group 1`	Displays real-time statistical and operational information for load balancing operations. If given without any options, this command displays information for the load balancing groups and each cable interface's current load and load balancing status.
Step 5	**show cable modem** [*ip-address* | *mac-address* | **cable** *slot/port* [**upstream** *port*] | **name** *fqdn*] [*verbose*] **Example:** `Router# show cable modem 40.3.160.15 verbose`	Displays information for the registered and unregistered CMs.

Examples

Use the **show cable load-balance docsis-group** command to see the DOCSIS group status and to see the list of modems in the group, use the **show cable fiber-node** command to see the information on fiber nodes, use the **show cable load-balance** command to see information on LBG and DOCSIS channels, and use the **show cable modem** command to see the information on all the CMs.

The following examples show the output of the **show cable load-balance docsis-group** command:

```
Router# show cable load-balance docsis-group 2
DOCSIS LB Enabled: Yes
DOCSIS     Group Status Interval DCC mask  Policy     Method Threshold
Group      Index                /UCC                  DS/US  M/E/U/P/S
2          82    RE 10       0xF8(0)/N 0          s/s    1/1/70/70/50
Router# show cable load-balance docsis-group 1 modem-list
US                    Group Index Mac Address      Priority
Mo1/0/0:0/U0          81          (1)
                                  0000.ca45.9898   0
Mo1/0/0:0/U1          81          (0)
Mo1/0/0:0/U2          81          (2)
                                  0013.711c.0820   0
                                  0016.924f.8300   0
```

Effective from Cisco IOS Release 12.2(33)SCH, the output of the **show cable load-balance docsis-group** command is modified to include an additional field MUPFXLR to display more status information on the modems in the DOCSIS groups. For more information, see the Cisco IOS CMTS Cable Command Reference.

The following example shows the modified output of the **show cable load-balance docsis-group** command:

```
Router#show cable load docsis-group fn 1 md c6/0/0 modem-list
Load for five secs: 1%/0%; one minute: 2%; five minutes: 1%
Time source is NTP, 13:39:31.300 PDT Thu Mar 28 2013
Codes: M - Multicast, U - UGS, P - PCMM, F - Max-Failures, X - eXcluded
       L - L2vpn, R - RSVP
Primary DS     Grp Idx MAC Address    RCC-ID Bad Rfid Priority MUPFXLR
In6/0/0:0/UB   40448   (6)
                       e448.c70c.98af 1               2        -------
                       e448.c70c.9b76 1               2        -------
                       e448.c70c.9c15 1               2        -------
                       e448.c70c.9a92 1               2        -------
                       e448.c70c.99e4 1               2        -------
                       e448.c70c.9a35 1               2        -------
In6/0/0:0/U0   40448   (0)
In6/0/0:0/U1   40448   (1)
                       e448.c70c.9915                 2        -------
In6/0/0:0/U2   40448   (0)
In6/0/0:0/U3   40448   (0)
In6/0/0:1/UB   40448   (5)
                       e448.c70c.9abc 1               2        -------
                       e448.c70c.993f 1               2        -------
                       e448.c70c.9927 1               2        -------
                       e448.c70c.9b82 1               2        -------
                       4458.2945.2cb8 1               2        -------
In6/0/0:1/U0   40448   (0)
In6/0/0:1/U1   40448   (0)
In6/0/0:1/U2   40448   (0)
In6/0/0:1/U3   40448   (0)
In6/0/0:2/UB   40448   (5)
                       e448.c70c.9759 1               2        -------
                       e448.c70c.9a0e 1               2        -------
                       e448.c70c.992d 1               2        -------
                       e448.c70c.9a38 1               2        -------
                       0025.2ed9.9984 1               2        -----L-
In6/0/0:2/U0   40448   (0)
In6/0/0:2/U1   40448   (0)
In6/0/0:2/U2   40448   (0)
In6/0/0:2/U3   40448   (0)
```

```
In6/0/0:3/UB   40448   (5)
                       e448.c70c.9c00 1               2        -------
                       e448.c70c.99a5 1               2        -------
                       e448.c70c.9a5f 1               2        -------
                       e448.c70c.9a3b 1               2        -------
                       e448.c70c.96b1 1               2        -------
In6/0/0:3/U0   40448   (0)
In6/0/0:3/U1   40448   (0)
In6/0/0:3/U2   40448   (0)
In6/0/0:3/U3   40448   (0)
```

The following example shows the output of the **show cable fiber-node** command:

```
Router# show cable fiber-node
Fiber-Node         Config Status
Fiber-Node 1
       Modular-Cable 1/0/0:  0-1
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
```

The following examples show the output of the **show cable load-balance** command:

```
Router#show cable load-balance
Group  Interval  Method         DCC Init   Threshold
                                Technique  Minimum  Static  Enforce  Ugs   PCMM
1      10        service-flows 1          1        2%      2%       ---   ---
2      10        modems        0          5        10%     ---      ---   ---

DOCSIS LB Enabled: No
Router# show cable load-balance load
Interface             State      Group  Utilization  Reserved Modems Flows Weight
                                 Index
Cable5/0/3 (459 MHz) up         1      0%(0%/0%)       0%    7      7     37
Cable5/0/3/U0        up         1      0%              0%    2      2     1.2
Cable5/0/3/U1        up         1      0%              0%    2      2     1.2
Cable5/0/3/U2        up         1      0%              0%    2      2     1.2
Cable5/0/3/U3        up         1      0%              0%    1      1     1.2
Cable5/0/4 (465 MHz) up         1      0%(0%/0%)       0%    7      7     37
Cable5/0/4/U0        up         1      0%              0%    1      1     1.2
Cable5/0/4/U1        up         1      0%              0%    2      2     1.2
Cable5/0/4/U2        up         1      0%              0%    2      2     1.2
Cable5/0/4/U3        up         1      0%              0%    2      2     1.2
Mo1/0/0:0 (555 MHz)  down       1      0%(0%/0%)       0%    0      0     0
Router# show cable load-balance fiber-node-validation
DOCSIS LBG ID    Match    Channel    Fiber-node list
1                match    Ca5/0/0/U0 {1}
                          Ca5/0/0/U1 {1}
                          Ca5/0/0/U2 {1}
                          Ca5/0/0/U3 {1}
                          Mo1/0/0:0  {1}
                          Mo1/0/0:1  {1}
2                mismatch Ca5/0/0/U0 {1}
                          Ca5/0/0/U1 {1}
                          Ca5/0/0/U2 {1}
                          Ca5/0/0/U3 {1}
                          Ca5/0/0    {}
```

The following example shows the output of the **show cable modem** command:

```
Router# show cable modem 40.3.160.19 verbose
LB group ID assigned(index)        : 1(81)
LB group ID in config file(index)  : N/A(N/A)
LB policy ID  : 0
LB policy ID in config file        : 0
LB priority                        : 0
Tag                                :
```

In Cisco IOS Release 12.2(33)SCF, DOCSIS 3.0 GLBG is generated dynamically by the fiber node configuration, if a valid fiber node is configured.

For example, if the fiber node configuration is:

```
cable fiber-node 2
 downstream Modular-Cable 1/0/0 rf-channel 0-3
 downstream Cable7/0/0
 upstream Cable 7/0 connector 0-3
!
```

The GLBG generated by this fiber node is similar to:

```
Router# show cable load-balance docsis-group fn 2 md cable 7/0/0
DOCSIS 3.0 General LB
MD       FN  Group S Intv DCC mask  Policy     Mtd MD-CM-SG Threshold
             Index       /UCC                  D/U          M/E/U/P/S
Ca7/0/0  2   48129 E 30   0xF8(0)/N 0          m/m 0x3C0101 5/10/70/70/50



Router# show cable load-balance docsis-group fn 2 md cable 7/0/0 all
DOCSIS 3.0 General LB
MD       FN  Group S Intv DCC mask  Policy     Mtd MD-CM-SG Threshold
             Index       /UCC                  D/U          M/E/U/P/S
Ca7/0/0  2   48129 E 30   0xF8(0)/N 0          m/m 0x3C0101 5/10/70/70/50
Current load:
DOCSIS load-balancing load
Interface            State   Group  Utilization Rsvd NBCM  WB/UB Flows Weight
                             Index                    Total Total
Cable7/0/0 (333 MHz) up      48129  0%(0%/0%)    0%   2     8     7     37
Cable7/0/0/U0        up      48129  0%           0%   22    7     29    7.6
Cable7/0/0/U1        up      48129  0%           0%   21    8     28    7.6
Cable7/0/0/U2        up      48129  0%           0%   21    8     28    7.6
Cable7/0/0/U3        up      48129  0%           0%   20    10    30    7.6
Mo1/0/0:0 (501 MHz)  up      48129  0%(0%/0%)    0%   2     63    2     36
Mo1/0/0:0/U0         up      48129  0%           0%   22    7     29    7.6
Mo1/0/0:0/U1         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:0/U2         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:0/U3         up      48129  0%           0%   20    10    30    7.6
Mo1/0/0:1 (507 MHz)  up      48129  0%(0%/0%)    0%   1     58    1     36
Mo1/0/0:1/U0         up      48129  0%           0%   22    7     29    7.6
Mo1/0/0:1/U1         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:1/U2         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:1/U3         up      48129  0%           0%   20    10    30    7.6
Mo1/0/0:2 (513 MHz)  up      48129  0%(0%/0%)    0%   2     59    2     36
Mo1/0/0:2/U0         up      48129  0%           0%   22    7     29    7.6
Mo1/0/0:2/U1         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:2/U2         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:2/U3         up      48129  0%           0%   20    10    30    7.6
Mo1/0/0:3 (519 MHz)  up      48129  0%(0%/0%)    0%   1     61    1     36
Mo1/0/0:3/U0         up      48129  0%           0%   22    7     29    7.6
Mo1/0/0:3/U1         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:3/U2         up      48129  0%           0%   21    8     28    7.6
Mo1/0/0:3/U3         up      48129  0%           0%   20    10    30    7.6
Target assignments:
Interface            State      Group   Target
                                Index
Cable7/0/0 (333 MHz) up         48129
Cable7/0/0/U0        up         48129
Cable7/0/0/U1        up         48129
Cable7/0/0/U2        up         48129
Cable7/0/0/U3        up         48129
Mo1/0/0:0 (501 MHz)  up         48129   Mo1/0/0:1 (507 MHz)
Mo1/0/0:0/U0         up         48129
Mo1/0/0:0/U1         up         48129
Mo1/0/0:0/U2         up         48129
```

```
Mo1/0/0:0/U3          up          48129
Mo1/0/0:1 (507 MHz)   up          48129
Mo1/0/0:1/U0          up          48129
Mo1/0/0:1/U1          up          48129
Mo1/0/0:1/U2          up          48129
Mo1/0/0:1/U3          up          48129
Mo1/0/0:2 (513 MHz)   up          48129
Mo1/0/0:2/U0          up          48129
Mo1/0/0:2/U1          up          48129
Mo1/0/0:2/U2          up          48129
Mo1/0/0:2/U3          up          48129
Mo1/0/0:3 (519 MHz)   up          48129
Mo1/0/0:3/U0          up          48129
Mo1/0/0:3/U1          up          48129
Mo1/0/0:3/U2          up          48129
Mo1/0/0:3/U3          up          48129
Statistics:
Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable7/0/0 (333 MHz)   up         8         0         0         0
Cable7/0/0/U0          up         30        0         0         0
Cable7/0/0/U1          up         83        0         0         0
Cable7/0/0/U2          up         48        0         0         0
Cable7/0/0/U3          up         34        0         0         0
Mo1/0/0:0 (501 MHz)    up         19        0         0         0
Mo1/0/0:0/U0           up         33        0         0         0
Mo1/0/0:0/U1           up         46        0         0         0
Mo1/0/0:0/U2           up         22        0         0         0
Mo1/0/0:0/U3           up         22        0         0         0
Mo1/0/0:1 (507 MHz)    up         22        0         0         0
Mo1/0/0:1/U0           up         9         0         0         0
Mo1/0/0:1/U1           up         19        0         0         0
Mo1/0/0:1/U2           up         15        0         0         0
Mo1/0/0:1/U3           up         21        0         0         0
Mo1/0/0:2 (513 MHz)    up         21        0         0         0
Mo1/0/0:2/U0           up         4         0         0         0
Mo1/0/0:2/U1           up         3         0         0         0
Mo1/0/0:2/U2           up         6         0         0         0
Mo1/0/0:2/U3           up         7         0         0         0
Mo1/0/0:3 (519 MHz)    up         9         0         0         0
Mo1/0/0:3/U0           up         1         0         0         0
Mo1/0/0:3/U1           up         2         0         0         0
Mo1/0/0:3/U2           up         4         0         0         0
Mo1/0/0:3/U3           up         4         0         0         0
Pending:
Modem          Grp Idx Primary RF/RCC              MD/TCS        Action Active Retries
                       Src           Target       Src    Target         Time
```

Additional References

The following sections provide references related to the Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing feature.

Related Documents

Related Topic	Document Title
Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change	Load Balancing, Dynamic Channel Change, and Dynamic Bonding Change on the Cisco CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_load-bal_dcc.html

Related Topic	Document Title
Cable commands	Cisco IOS CMTS Cable Command Reference, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/ reference/cbl_book.html

Standards and RFCs

Standards	Title
CM-SP-MULPIv3.0-I09-090121	Data-Over-Cable Service Interface Specifications MAC and Upper Layer Protocols Interface Specification

MIBs

MIB	MIBs Link
• DOCS-LOADBALANCING-MIB • DOCS-LOADBAL3-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

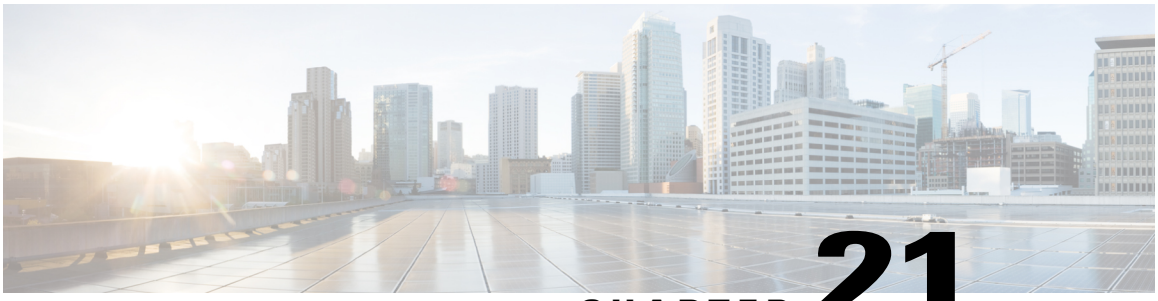
Table 51: Feature Information for Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing

Feature Name	Releases	Feature Information
Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing	12.2(33)SCC	

Feature Name	Releases	Feature Information
		In Cisco IOS Release 12.2(33)SCC, this feature was introduced on Cisco uBR10012 routers. The following section provide information about this feature: • Information About Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing, on page 497 • The following commands were introduced or modified: ◦ **cable load-balance docsis-group** ◦ **cable load-balance d30-ggrp-default** ◦ **cable load-balance modem max-failures** ◦ **cable load-balance restrict modem** ◦ **cable tag** ◦ **show cable load-balance docsis-group** ◦ **show cable fiber-node** ◦ **cable load-balance docsis-enable** ◦ **docsis-policy** ◦ **docsis-version** ◦ **downstream** ◦ **init-tech-list** ◦ **init-tech-ovr** ◦ **interval** ◦ **method** ◦ **name** ◦ **oui** ◦ **override** ◦ **policy** ◦ **restricted**

Feature Name	Releases	Feature Information
		◦ **service-class (cmts-tag)** ◦ **service-type-id** ◦ **service-type-id (cmts-tag)** ◦ **tag** ◦ **threshold**
		• **upstream (config-lb-group)** • **cable load-balance rule** • **show cable load-balance** • **cable load-balance docsis-policy**
Restricted/General Load Balancing and Narrowband Dynamic Bandwidth Sharing with Downstream Dynamic Load Balancing	12.2(33)SCD	In Cisco IOS Release 12.2(33)SCD, this feature was introduced on Cisco uBR7200 series routers.
DOCSIS 2.0 multicast enhancement for VDOC.	12.2(33)SCD5	This feature enables the customer to tune a DOCSIS 2.0 cable modem to a specific downstream having static multicast video forwarding on it. The following command was modified: • **cable load-balance rule**
Channel Assignment for RLBG/GLBG	12.2(33)SCF	RLBG/GLBG channel assignment varies for different DOCSIS versions of cable modems. The following command was modified: • **show cable load-balance docsis-group**
Handling of Channel Assignment	12.2(33)SCF1	Handling of channel assignment when an LBG is disabled, is changed.
Auto-generate DOCSIS 2.0 GLBG	12.2(33)SCH	Generates GLBG automatically for DOCSIS 2.0 fiber node configurations. The following command was introduced: **cable load-balance d20 GLBG auto-generate**

Feature Name	Releases	Feature Information
Independent Upstream/Downstream Throughput Rules	12.2(33)SCH	Support for independent checking for upstream or downstream rules for load balancing. For upstream load balancing, upstream throughput rules are checked, and for downstream load balancing, downstream throughput rules are checked.
TLV type Tag	12.2(33)SCH	Configures a TLV type matching rule. The following command was modified: **cable tag** The following command was introduced: **tlv**



CHAPTER 21

RSVP-Based Video on Demand Support Over DOCSIS

First Published: December 17, 2008

The Cisco universal broadband router supports Video on Demand (VoD) over DOCSIS (Data Over Cable Service Interface Specification) services using a Resource ReSerVation Protocol (RSVP) bandwidth request from the VoD server. RSVP is used by the Cable Modem Termination System (CMTS) to request video data from the network for specific application data flows.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring RSVP-Based Video on Demand Support Over DOCSIS

The table below shows the hardware compatibility prerequisites for RSVP-Based video on demand support over DOCSIS.

Table 52: Cable Hardware Compatibility Matrix for RSVP-Based Video on Demand Support Over DOCSIS

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco uBR10-MC5X20S/U/H

The software prerequisites for the RSVP-based video on demand support over DOCSIS are:

- This feature does not require DOCSIS3.0 setup.
- The cable modems should be compliant with DOCSIS 1.1 or higher.
- The **ip rsvp bandwidth** command on the cable bundle interface should provide actual reserved bandwidth available.
- This feature is supported on all CMTS platforms.
- The **ip rsvp bandwidth** command should be configured on the WAN interface on the CMTS.
- IP routing is configured on CMTS so that the bundle interface can be reached from the video source.

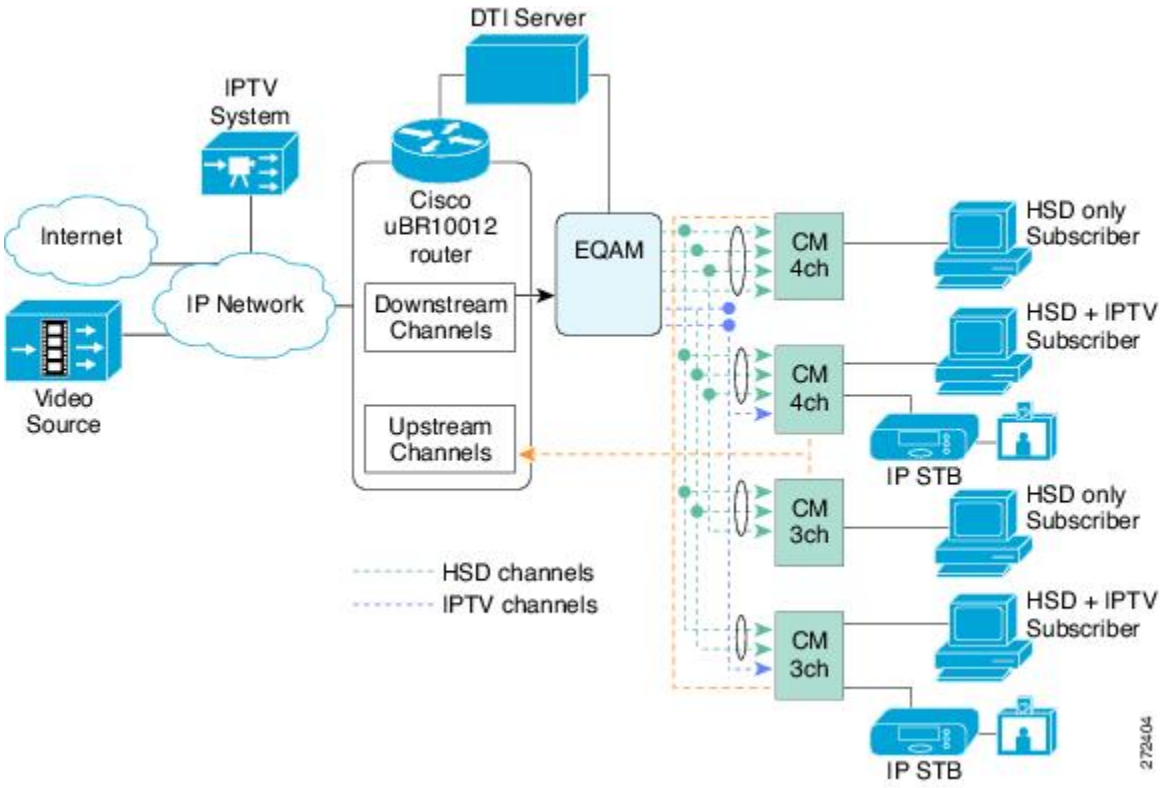
Restrictions for Configuring RSVP-Based Video on Demand Support Over DOCSIS

- RSVP implementation supports IPv4 only.
- Upstream service flow creation is not supported.
- RSVP receiver proxy supports controlled-load service only.
- RSVP over MPLS VPN is not supported.

Information About RSVP-Based Video on Demand Support Over DOCSIS

RSVP is used by a host to request specific quality of service (QoS) from the network for particular application data streams or flows. RSVP is used by the CMTS to deliver video requests along the data path of the flows and maintains the state to provide the requested service. RSVP requests generally result in resources being reserved in each node along the data path.

Figure 7: Configuring RSVP-Based Video on Demand Support Over DOCSIS



The following process is used to reserve DOCSIS resources on CMTS based on RSVP:

1. The CMTS intercepts the RSVP requests that are intended for the set-top boxes in the CMTS service area and reserves DOCSIS resources.
2. When a path message reaches the CMTS, it determines the DOCSIS resources required.
3. The CMTS creates a service flow and classifier to the cable modem.
4. The CMTS responds with a RSVP reserve message in the direction of the streamer.

How to Configure RSVP-Based Video over DOCSIS

This section describes the configuration tasks that are performed when using the RSVP-based video over DOCSIS feature on the Cisco CMTS platforms. You can use the command-line interface (CLI) commands to complete the configuration.

Configuring the RSVP Service Class

To specify the default service class for RSVP, use the **cable rsvp default-scn** command in global configuration mode. This command is used to specify DOCSIS service flow parameters such as activity time-out and service-flow attribute mask.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rsvp default-scn** *service-class name* **Example:** `Router(config)# cable rsvp default-scn RSVPClass`	Specifies the default service class for RSVP. • *service-class name*— The DOCSIS service class name.

Displaying the RSVP-DOCSIS Flow Data

The RSVP-DOCSIS flow data contains details of the RSVP session and DOCSIS service flow identifier data structure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**show cable rsvp flow-db** [*mac-addr*] **Example:** `Router(config)# show cable rsvp flow-db`	Displays contents of the RSVP to DOCSIS service flow mapping database. • *mac-addr*—(Optional) The MAC address of the specific cable modem in hexadecimal format.

	Command or Action	Purpose

Additional References

The following sections provide references related to configuring RSVP-based Video over DOCSIS.

Related Documents

Related Topic	Document Title
CMTS cable commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_release_notes_list.html

Standards and RFCs

RFC	Title
RFC 2205	Resource ReSerVation Protocol
RFC 2210	The Use of RSVP with IETF Integrated Services

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

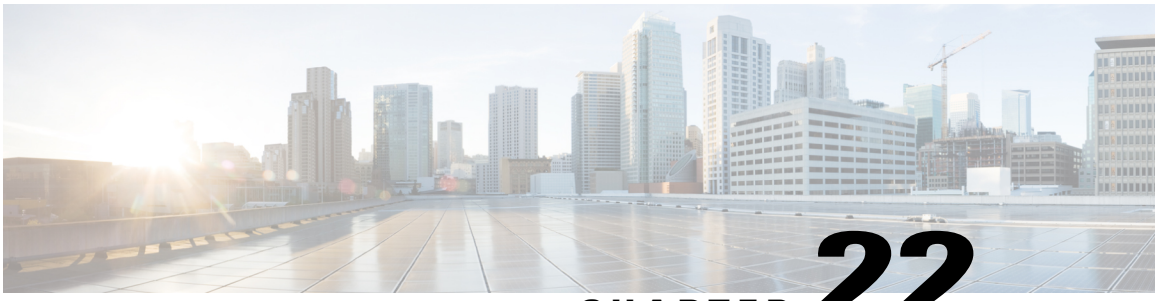
Feature Information for RSVP-Based Video over DOCSIS

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 53: Feature Information for RSVP-Based Video over DOCSIS

Feature Name	Releases	Feature Information
RSVP-Based Video on Demand Support Over DOCSIS	12.2(33)SCB	The Cisco universal broadband router supports VoD over DOCSIS services using a RSVP bandwidth request from the VoD server. RSVP is used by the CMTS to request video data from the network for specific application data flows. The following sections provide information about this feature: • Configuring the RSVP Service Class, on page 534 • Displaying the RSVP-DOCSIS Flow Data, on page 534



CHAPTER 22

S-CDMA and Logical Channel Support on the Cisco CMTS Routers

First Published: November 9, 2009

Last Updated: November 29, 2010

Cisco IOS Release 12.2(33)SCC introduces the S-CDMA and Logical Channel Support feature, which provides support for Synchronous Code Division Multiple Access (S-CDMA) upstream modulation profiles and logical channels on the Cisco cable modem termination systems (CMTS) routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for S-CDMA and Logical Channel Support

The table below shows the hardware compatibility prerequisites for this feature.

Table 54: S-CDMA and Logical Channel Support for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR10-MC5X20H[35] • Cisco UBR-MC20X20V[36] Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [37]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[38]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[39]

35 The S-CDMA feature is not supported on the Cisco uBR10-MC5X20H cable interface line card.

36 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

37 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

38 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

39 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Note Any reference to the Cisco UBR-MC20X20V cable interface line card used in this document is also applicable to its three variants—Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D.

- The cable physical plant must be capable of supporting the higher bandwidth S-CDMA modulation profiles.

- DOCSIS 2.0 compliant cable modems (CMs).
- DOCSIS 1.0 or DOCSIS 1.1 provisioned DOCSIS configuration file.
- Upstream configured for DOCSIS 2.0 S-CDMA or DOCSIS 3.0 S-CDMA mode.
- Complete a basic configuration of the Cisco uBR10012 router; this includes, at a minimum, the following tasks:
  - Configure a host name and password for the router.
  - Configure the router to support Internet Protocol (IP) operations.
  - Install and configure at least one Wide Area Network (WAN) adapter to provide backbone connectivity.
- Determine a channel plan for your router and all of its cable interfaces.
- Verify that your headend site includes all necessary servers to support DOCSIS and Internet connectivity, including Dynamic Host Configuration Protocol (DHCP), Time of Day (ToD), and Trivial File Transfer Protocol (TFTP) servers.
- The system clock on the router should be set to the current date and time to ensure that the system logs have the proper timestamp and the Baseline Privacy Interface Plus (BPI+) subsystem uses the correct timestamp for verifying cable modem digital certificates.

Restrictions for S-CDMA and Logical Channel Support

The S-CDMA feature has the following restrictions and limitations:

- The S-CDMA feature is not supported on the Cisco uBR10-MC5X20H cable interface line card.
- DOCSIS 1.0 provisioned CM configuration file is not recommended or allowed for cable modems on the S-CDMA channel.
- The Cisco IOS Release 12.2(33)SCC supports a maximum of 10 modulation profiles for each of the DOCSIS 2.0 A-TDMA and S-CDMA modes. However, if you enable the global modulation profile there is no restriction on the number of modulation profiles you can use, and can assign any modulation profile number to any DOCSIS mode.
- Advanced hardware-based spectrum management features (such as guided frequency hopping, dynamic upstream modulation, and proactive carrier-to-noise ratio [CNR] based frequency hopping and channel width changes) are not supported for S-CDMA upstreams.
- Changing the DOCSIS mode of an upstream takes all cable modems on that upstream offline, which forces the cable modems to reregister, so that the CMTS can determine the capabilities of the cable modems on the new channels.
- For the S-CDMA high availability, there should be timestamp, minislot, and frame counters synchronization between the working and the protect line cards.
- The DOCSIS 3.0 option scdma-d3 (4SR) is available only when the CMTS is configured to operate in the global modulation profile format.
- If you revert to the legacy modulation profile from the global modulation profile, all the modulation profiles that are outside of the legacy number space range are lost.

The Logical Channel Support feature has the following restrictions and limitations:

- The CMTS must support the logical channel types 3S and 4SR individually on the Cisco uBR-MC88V cable interface line card.
- The Cisco uBR10-MC5X20H, Cisco UBR-MC20X20V, and Cisco uBR-MC88Vcable interface line cards can only support up to two logical channels per physical port.
- The upstream bonding at the logical channel level is supported with the following limitations:
  - The upstream bonding of the logical channels from the same physical port (on the same radio frequency spectrum) is not allowed.
  - The upstream bonding is available only to the first logical channel on each physical port.
- Admission control policy cannot be configured at the logical channel level.
- Load balancing is restricted only to the first logical channel. However, the secondary logical channel can be selected as the source channel and not the target channel. That is, load balancing can only move modems from the secondary logical channel, and not to the secondary logical channel.

Information About S-CDMA and Logical Channel Support

The following sections describe the S-CDMA and Logical Channel Support feature:

S-CDMA Services

S-CDMA provides a number of advanced physical layer (PHY) capabilities as per the new DOCSIS 3.0 specifications, which improves the maximum upstream bandwidth on cable networks.

The S-CDMA feature allows the same physical RF upstream channel to receive multiple bursts simultaneously. It uses a two-dimensional (time and code) data transmission technique where multiple modems can simultaneously send their data, each using their own codes, in the same time slot. The codes are orthogonal in nature and do not interfere with each other.

Data is sent over an array of up to 128 spreading codes and all modems are required to transmit their data at precisely the same time. This means that the CMTS and modems have to be synchronized at the symbol clock level (known as synchronous CDMA).

A burst from a particular cable modem may be transmitted on two or more codes (out of the available 128 codes) in one or more frames. A frame can contain bursts transmitted simultaneously from multiple CMs (each on a separate subset of codes) defined as per MAP messages.

The S-CDMA feature allows cable system operators to utilize parts of the upstream below 20 MHz that was previously unusable due to noise conditions. This type of noise cannot be removed with the ingress noise cancellation technology available as part of the DOCSIS 2.0 standard.

The S-CDMA feature incorporates the following advantages and improvements on DOCSIS 3.0 networks:

- Upstreams can be configured for two different modes to support different mixes of cable modems:
  - S-CDMA mode to support DOCSIS 2.0 cable modems.
  - S-CDMA-d3 mode to support DOCSIS 3.0 cable modems.

- S-CDMA-d3 mode allows DOCSIS 3.0 modems to use all data interval usage codes (IUC) like IUC 5, 6, 9, 10, and 11 for data bursts.
- S-CDMA mode of operation provides higher bandwidth on the upstream using 64-QAM, 32-QAM, 16-QAM, 8-QAM, and QPSK modulation profiles.

The table below shows the maximum data rates supported on S-CDMA.

Table 55: Maximum S-CDMA Data Rates

Upstream Channel Width	Modulation Scheme	Baud Rate Sym/sec	Maximum Raw Bit Rate Mbit/sec
6.4 MHz	64-QAM	5.12 M	30.72
	32-QAM		25.60
	16-QAM		20.48
	8-QAM		15.36
	QPSK		10.24
3.2 MHz	64-QAM	2.56 M	15.36
	32-QAM		12.80
	16-QAM		10.24
	8-QAM		7.68
	QPSK		5.12
1.6 MHz	64-QAM	1.28 M	7.68
	32-QAM		6.40
	16-QAM		5.12
	8-QAM		3.84
	QPSK		2.56

Modulation Profiles

To simplify the administration of Advanced Time Division Multiple Access (A-TDMA) and S-CDMA modulation profiles, the S-CDMA feature provides a number of preconfigured modulation profiles that are optimized for different modulation schemes. We recommend using these preconfigured profiles.

Each mode of operation also defines a default modulation profile that is automatically used when a profile is not specifically assigned to an upstream. These default modulation profiles (321 and 381) cannot be deleted.

A new global modulation profile is introduced in Cisco IOS Release 12.2(33)SCC, which allows you to assign any modulation profile number to any DOCSIS mode.

The table below lists the valid modulation profile ranges according to the cable interface and modulation type:

Table 56: Allowable Ranges for Modulation Profiles

Cable Interface	DOCSIS 2.0 (S-CDMA)	DOCSIS 3.0 (S-CDMA)
Cisco UBR-MC20X20V	321 to 330 (default is 321)	1 to 400 (default is 381)
Cisco uBR-MC88V	321 to 330 (default is 321)	1 to 400 (default is 381)

Global Modulation Profile

Cisco IOS Release 12.2(33)SCC introduces the global modulation profile scheme, which allows you to assign any modulation profile number to any DOCSIS mode up to 400. It eliminates the number space restriction and increases the number of modulation profiles that can be created per DOCSIS mode. Currently, there is a restriction of 10 modulation profiles per DOCSIS mode.

In global modulation profile scheme, you can assign any number between 1 to 400 to any modulation profiles. The global modulation profile mode allows you to create and configure DOCSIS 3.0 channel type 4SR (scdma-d3). When the DOCSIS mode of an upstream is changed into scdma-d3, it is initially assigned to the system created default modulation profile as shown in Table 56: Allowable Ranges for Modulation Profiles , on page 544.

Note Though you can assign any number between 1 to 400 to any modulation profile, the default modulation profile number assigned to an upstream channel for a given channel type will remain the same. That is, modulation profile numbers 21, 121, 221, 321, and 381 will be applicable for TDMA, mixed, A-TDMA, S-CDMA, and DOCSIS 3.0 S-CDMA channel types.

All the existing and previously defined modulation profiles are converted to the new format. However, all the newly created modulation profiles, which are outside of the legacy number space range, will be lost when you revert to the legacy modulation profile.

The new global modulation profile scheme is enabled using the cable modulation-profile global-scheme command. For more details on this command, refer to the Cisco IOS CMTS Cable Command Reference .

Benefits

The S-CDMA feature provides the following benefits:

- Provides full compatibility with DOCSIS 2.0 and DOCSIS 3.0 cable modems (CMs) and cable modem termination systems (CMTS).
- Increases protection against electronic impairments that occur in cable systems, allowing for a more robust operating environment.
- Supports S-CDMA ingress noise cancellation technology that provide more knobs for fine tuning.
- Supports all existing upstream bonding capabilities for Time Division Multiple Access (TDMA) and A-TDMA channels under S-CDMA.
- Supports up to two logical channel combinations for the Cisco UBR-MC20X20V and Cisco uBR-MC8X8V cable interface line cards.
- Supports the In-Service Software Upgrade (ISSU) feature.

Logical Channels

The concept of a logical channel refers to time-division multiplexing (TDM) of the same radio frequency (RF) spectrum allocated to one physical upstream port. All logical upstream channels defined within the physical upstream port share the same upstream RF spectrum or the bandwidth. The MAC-scheduler is responsible for managing how that common bandwidth is shared or distributed.

Using the Logical Channel Support feature, cable system operators can segment and time-multiplex one spectrum for supporting the legacy modems, near and far modems, and newer DOCSIS 3.0 modems with various service levels.

The Logical Channel Support feature provides the following benefits to cable service providers and their partners and customers:

- Switchovers between the same cable interface line cards at the logical channel level, as part of high availability (HA). For example, switchover from Cisco uBR10-MC5X20H line card to Cisco uBR10-MC5X20H line card is supported.
- Support for the In-Service Software Upgrade (ISSU) feature.

Each logical channel has its own Upstream Channel ID, upstream channel descriptor (UCD) messages, and Mini-slot Allocation Packet (MAP) messages. The logical channels on their own must satisfy the ranging and UCD change requirements that are imposed on a legacy standalone upstream channel.

The Cisco uBR10-MC5X20H and Cisco UBR-MC20X20V cable interface line cards support two logical channel combinations per physical port.

When two logical channels are configured through the **cable upstream max-logical-chans** command, both logical channels are mapped to the same physical port specified and the physical upstream bandwidth is shared between the two logical channels. However, from the cable modem perspective, each logical channel appears as an independent upstream channel.

When multiple logical channels are configured, the upstream-related commands are categorized into physical port level and logical channel level groups. Logical channel level commands use the format of **cable upstream** *n m,* where *n* denotes the physical port number, and *m* denotes the logical channel index number.

For more details on the **cable upstream max-logical-chans** command, refer to the Cisco IOS CMTS Cable Command Reference .

Spectrum Management on Logical Channels

Spectrum management allows you to prevent long-term service interruptions caused by upstream noise events in the cable plant. Spectrum management is also used for fault management and troubleshooting the cable network.

The Logical Channel Support feature supports all the basic spectrum management features. Some spectrum management features operate on the physical port level while others operate at the logical channel level.

The spectrum group assignment feature operates at the physical port level, and the Dynamic Upstream Modulation feature using Signal-to-Noise Ratio (SNR) operates at the logical channel level.

For more information on spectrum management, refer to the *Spectrum Management and Advanced Spectrum Management for the Cisco CMTS Routers* document at the following location: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_spctrm_mgt.html

Load Balancing on Logical Channels

The Load Balancing (LB) feature allows cable system operators to distribute cable modems across RF downstream and upstream channels on the same cable interface line card, or across multiple cable interface line cards in some circumstances. Load balancing maximizes bandwidth and usage of the cable plant.

Load balancing is supported on logical channels using a two-tiered approach—the first level uses the traditional load balancing to move modems between the physical channels, and the second level moves modems amongst the logical channels.

The first level of load balancing (known as Cisco LB implementation) moves the modems amongst the physical upstream channels, identified in the load balancing group. It uses the aggregate upstream channel utilization statistics of a physical channel, including that of all logical channels, to perform load balancing.

The second level of load balancing moves modems among the logical channels defined within a physical channel (no outside moves). It is referred to as "per CM spectrum management" as it is strictly based on the physical channel parameters or conditions, or the physical layer capabilities of the CM.

For more information on the LB feature, refer to the *Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers* document at the following location: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_load-bal_dcc.html

How to Configure S-CDMA and Logical Channel Support

This section describes the following tasks that are required to implement S-CDMA and Logical Channel Support:

Creating Modulation Profiles

This section describes how to create modulation profiles for the different modes of DOCSIS operations, using the preconfigured modulation profile options.

Note You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.

Creating a DOCSIS 2.0 S-CDMA Modulation Profile

This section describes how to create a modulation profile for the DOCSIS 2.0 S-CDMA mode of operation, using one of the preconfigured modulation profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* **qam-16** **Example:** `Router(config)# cable modulation-profile 322 qam-16`	Creates a preconfigured modulation profile, where the burst parameters are set to their default values for each burst type: • *profile* —Modulation profile number. The valid range is from 321 to 330. The system creates profile 321 as the default modulation profile. • **qam-16—**Default 16-QAM profile.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Global Modulation Profile

This section describes how to enable or configure a global modulation profile. The global modulation profile scheme eliminates the number space restriction associated with the legacy mode allowing you to assign any number between 1 to 400 to any modulation profiles.

Note When you configure a global modulation profile, all the previous modulation profiles are automatically converted. However, when you revert back to the legacy mode, all the profiles that are outside of the legacy number space range are lost.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile global-scheme** **Example:** `Router(config)# cable modulation-profile global-scheme`	Activates the global modulation profile scheme, where you can assign any number between 1 to 400 to any modulation profile.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Creating a DOCSIS 3.0 S-CDMA Modulation Profile

This section describes how to create a modulation profile for the DOCSIS 3.0 S-CDMA mode of operation, using one of the preconfigured modulation profiles.

Note The **scdma-d3** option is available only after configuring the CMTS to operate in the global modulation profile mode. This option is not available in the default mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* **scdma-d3 qam-16** **Example:** `Router(config)# cable modulation-profile 382 scdma-d3 qam-16`	Creates a preconfigured modulation profile, where the burst parameters are set to their default values for each burst type: • *profile*—Modulation profile number. The valid range is from 1 to 400. The system creates profile 381 as the default modulation profile. • **scdma-d3**—Configures the upstream only for DOCSIS 3.0 S-CDMA modulation profiles.

	Command or Action	Purpose
		• **qam-16—**Default 16-QAM profile.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the DOCSIS Mode and Profile on an Upstream

This section describes how to configure an upstream for a DOCSIS mode of operation, and then to assign a particular modulation profile to that upstream.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/port* | *slot/subslot/port*} **Example:** `Router(config)# interface cable 5/0/0`	Enters interface configuration mode for the indicated cable downstream interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ *slot*—3 to 6 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ *slot*—1 and 2 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are: ◦ *slot*—5 to 8 ◦ *subslot*—0 or 1 ◦ *port*—0 to 4 (depending on the cable interface)

	Command or Action	Purpose
Step 4	**cable upstream** *n* **docsis-mode** {**atdma** | **scdma** | **scdma-d3** | **tdma** | **tdma-atdma**} **Example:** `Router(config-if)# cable upstream 0 docsis-mode atdma`	Configures the upstream for the desired DOCSIS mode of operation: • *n* —Upstream port number. Valid values are 0 to 3 by default, but can be increased to a maximum of 7 using the cable upstream max-ports command. • **atdma—**Configures the upstream only for DOCSIS 2.0 A-TDMA modulation profiles. • **scdma—**Configures the upstream only for DOCSIS 2.0 S-CDMA modulation profiles. • **scdma-d3—**Configures the upstream only for DOCSIS 3.0 S-CDMA modulation profiles. • **tdma—**Configures the upstream only for DOCSIS 1.X TDMA modulation profiles. • **tdma-atdma—**Configures the upstream for both, A-TDMA, and TDMA operations (mixed mode). **Note** The **scdma-d3** mode is available only when the global modulation profile is used.
Step 5	**cable upstreamn** *n* **modulation-profile** *profile* [*profile2*] [*profile3*] **Example:** `Router(config-if)# cable upstream 0 modulation-profile 241`	Assigns the particular modulation profile to this upstream. • *profile*—Modulation profile used on this upstream. The valid range for the *profile* parameter depends on the current DOCSIS mode: ◦ If the upstream is configured for DOCSIS 2.0 S-CDMA, the valid range is from 321 to 330. ◦ If the upstream is configured for DOCSIS 3.0 S-CDMA mode, the valid range is from 1 to 400. • *profile2* —(Optional) Secondary modulation profile that the interface uses when noise on the upstream increases to the point that the primary modulation profile can no longer be used. (The secondary profile should specify a more robust profile than the primary profile to cope with the noise.) • *profile3* —(Optional) Tertiary modulation profile that the interface uses when noise on the upstream increases to the point that the secondary modulation profile can no longer be used. **Note** The tertiary modulation profile is available only for the basic dynamic modulation. You cannot use the tertiary modulation profile when a spectrum group is defined for the upstream. **Note** The type of modulation profiles must match the DOCSIS mode configured (using the **cable upstream docsis-mode** command) for the upstream.

	Command or Action	Purpose
Step 6	**cable upstream** *n* **active-codes** *active-codes* **Example:** `Router(config-if)# cable upstream 0 active-codes 64`	(Optional) Configures the number of active codes on an upstream channel. • *active-codes* —Number of active codes. The valid values range from 64 to 128. The active-codes have a default value of 112, when ingress noise cancellation is enabled; and a default value of 128, when ingress noise cancellation is disabled.
Step 7	**cable upstream** *n* **channel-width** *first-choice-width* **Example:** `Router(config-if)# cable upstream 0 channel-width 3200000`	(Optional) Specifies an upstream channel width for an upstream port. • *first-choice-width*— Upstream channel width in hertz (Hz) . For valid values refer to the **cable upstream channel-width** command.
Step 8	**cable upstream** *n* **codes-per-minislot** *minislot-code* **Example:** `Router(config-if)# cable upstream 0 codes-per-minislot 8`	(Optional) Specifies the number of codes-per-minislot allowed on an upstream channel. • *minislot-code*—Number of codes-per-minislot. The valid values range from 2 to 32.
Step 9	**cable upstream** *n* **max-codes-per-subframe** *subframe-codes* **Example:** `Router(config-if)# cable upstream 0 max-codes-per-subframe 128`	(Optional) Specifies the upper limit that overrides the maximum value of codes-per-subframe defined in the individual modulation profile setting for an upstream channel. • *subframe-codes*—Number of codes-per-subframe. The valid values range from 1 to 128, with a default value of 2.
Step 10	**cable upstream** *n* **spreading-interval** *spreading-interval* **Example:** `Router(config-if)# cable upstream 0 spreading-interval 32`	(Optional) Specifies the spreading interval for S-CDMA channels on an upstream channel. • *spreading-interval*—Spreading interval for S-CDMA channels. The valid values range from 1 to 32, with a default value of 16.
Step 11	**cable upstream** *n* **equalization-coefficient** **Example:** `Router(config-if)# cable upstream 0 equalization-coefficient`	(Optional) Enables the use of a DOCSIS preequalization coefficient on an upstream.
Step 12	**cable upstream** *n* **ingress-noise-cancellation** *interval* **Example:** `Router(config-if)# cable upstream 0 ingress-noise-cancellation 400`	(Optional) Configures, in milliseconds, how often the cable interface line card should sample the signal on an upstream to correct any ingress noise that has appeared on that upstream. • *interval*—Sample interval. The valid range is from 10 to 3000 milliseconds, with a default value of 200 milliseconds. **Note** The ingress noise cancellation has to be disabled to use a default value of 128 for active-codes. When ingress noise cancellation is enabled, the active-codes has a default value of 112.

	Command or Action	Purpose
		Note Repeat Step 3, on page 549 through Step 12, on page 551 for each cable interface and upstream to be configured.
Step 13	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the Logical Channel Support

This section describes how to configure logical channels for the Cisco uBR10-MC5X20H and Cisco UBR-MC20X20V cable interface line cards.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/port* | *slot/subslot/port*} **Example:** `Router(config)# interface cable 5/0/0`	Enters interface configuration mode for the indicated cable downstream interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ *slot*—3 to 6 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ *slot*—1 and 2 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are: ◦ *slot*—5 to 8 ◦ *subslot*—0 or 1 ◦ *port*—0 to 4 (depending on the cable interface)

	Command or Action	Purpose
Step 4	**cable upstream** *n* **max-logical-chans** *num-of-logical-channels* **Example:** `Router(config-if)# cable upstream 0 max-logical-chans 2`	Creates the specified number of logical channels per port on an upstream channel. • *n*—Upstream port. Valid values start with 0 for the first upstream port on the cable interface line card, but can be increased to a maximum of 7. • *num-of-logical-channels*—Number of logical channels per port.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring the S-CDMA and Logical Channel Support

To monitor the S-CDMA and Logical Channel Support feature, use the following procedures:

Displaying Modulation Profiles

To display the modulation profiles that are currently defined on the CMTS, use the **show running-config** command as shown in the example:

```
Router# show running-config | begin cable modulation-profile

cable modulation-profile global-scheme
cable modulation-profile 222 atdma request 0 16 0 22 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma initial 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma station 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma a-short 6 76 6 22 64qam scrambler 152 no-dif8
cable modulation-profile 222 atdma a-long 9 232 0 22 64qam scrambler 152 no-dif8
cable modulation-profile 222 atdma a-ugs 9 232 0 22 64qam scrambler 152 no-diff8
cable modulation-profile 223 atdma request 0 16 0 22 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma initial 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma station 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma a-short 6 76 6 22 64qam scrambler 152 no-dif8
cable modulation-profile 223 atdma a-long 14 220 0 22 64qam scrambler 152 no-di8
cable modulation-profile 223 atdma a-ugs 14 220 0 22 64qam scrambler 152 no-dif8
cable modulation-profile 400 scdma-d3 request 0 16 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 initial 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 station 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 short 3 76 12 64qam scrambler 152 no-diffm
cable modulation-profile 400 scdma-d3 long 9 232 0 64qam scrambler 152 no-diff m
cable modulation-profile 400 scdma-d3 a-short 6 76 6 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 a-long 9 232 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 a-ugs 9 232 0 64qam scrambler 152 no-diffm
--More--
```

To display a specific modulation profile in detail, specify the profile number with the **show cable modulation-profile** command as shown in the example:

```
Router# show cable modulation-profile 381
```

```
Mod  IUC     Type  Pre Diff FEC  FEC  Scrmb  Max Guard Last Scrmb Pre   Pre   RS
                   len enco T    k    seed   B   time  CW         offst Type
                             BYTE BYTE       siz size  short
381  request qpsk  64  no   0x0  0x10 0x152  0   0     no   yes   0     qpsk0 n
381  initial qpsk  98  no   0x5  0x22 0x152  0   0     no   yes   0     qpsk0 n
381  station qpsk  98  no   0x5  0x22 0x152  0   0     no   yes   0     qpsk0 n
381  short   qpsk  64  no   0x3  0x4C 0x152  12  0     yes  yes   0     qpsk0 n
381  long    qpsk  64  no   0x9  0xE8 0x152  0   0     yes  yes   0     qpsk0 n
381  a-short 64qam 64  no   0x6  0x4C 0x152  6   0     yes  yes   0     qpsk1 n
381  a-long  64qam 64  no   0x9  0xE8 0x152  0   0     yes  yes   0     qpsk1 n
381  a-ugs   64qam 64  no   0x9  0xE8 0x152  0   0     yes  yes   0     qpsk1 n
```

Displaying Cable Modem Capabilities and Provisioning

To display the capabilities of the online cable modems and how the modems were provisioned, use the **show cable modem mac** command:

```
Router# show cable modem mac

MAC Address     MAC          Prim  Ver    QoS    Frag Concat PHS Priv DS    US
                State        Sid          Prov                        Saids Sids
0014.bfbe.4fc3  offline      1     DOC1.0 DOC1.0 no   no     yes      15    16
0014.bfbe.4f59  offline      2     DOC1.0 DOC1.0 no   no     yes      15    16
0018.6830.2813  offline      3     DOC1.0 DOC1.0 no   no     yes      15    16
001a.c3ff.d208  online       4     DOC2.0 DOC1.1 yes  no     yes      24    8
0014.bfbe.4fbb  w-online     7     DOC3.0 DOC1.1 yes  yes    yes      15    16
0014.bfbe.4f9b  w-online     8     DOC3.0 DOC1.1 yes  yes    yes      15    16
0014.bfbe.4efd  init(t)      9     DOC1.0 DOC1.0 no   yes    yes      15    16
0018.684a.3f46  online       10    DOC2.0 DOC1.1 yes  yes    yes      15    16
0014.bfbe.4086  init(t)      11    DOC1.0 DOC1.0 no   yes    yes      15    16
001a.c3ff.d53a  w-online     12    DOC3.0 DOC1.1 no   no     yes      24    8
```

To display how many cable modems of each DOCSIS type are online on each upstream, use the **show cable modem mac summary** command:

```
Router# show cable modem mac summary

                          Cable Modem Summary
                          -------------------
                        Mac Version                        QoS Provision Mode
Interface       Total   DOC3.0  DOC2.0  DOC1.1  DOC1.0   Reg/Online   DOC1.1  D0
Cable7/1/0/U0   4       0       1       0       3        1            1       0
Cable8/0/0/UB   1       1       0       0       0        1            1       0
Cable8/0/0/U0.0 2       0       1       0       1        1            1       0
Cable8/0/0/U2   1       0       1       0       0        1            1       0
Cable8/0/0/U3   1       0       1       0       0        1            1       0
Cable8/0/0/U0.1 1       0       0       0       1        0            0       0
```

Displaying the Logical Channel Support

To display the logical channels within the physical upstream port, use the **show cable modem** command without any options:

```
Router# show cable modem

                                                                          B D
MAC Address    IP Address      I/F        MAC          Prim  RxPwr  Timing Num P I
                                          State        Sid   (dBmv) Offset CPE I P
0014.bfbe.4f9b 1.60.0.6        C5/0/0/U0.0 online        1     1.00   1406   0   N N
0014.bfbe.4efd 1.60.0.2        C5/0/0/U0.1 online        637   1.00   1409   0   N N
0014.bfbe.4efa 1.60.0.3        C5/0/0/U1   online        635   1.00   1409   0   N N
```

The following example shows a typical output of the **show controllers cable** command for a cable interface line card that is configured with multiple logical channels:

```
Router# show controllers cable 7/1/0 upstream 0
 Cable7/1/0 Upstream 0 is up
```

```
Frequency 10.000 MHz, Channel Width 6.400 MHz, Symbol Rate 5.120 Msps
Modulations - A-short 64-QAM, A-long 64-QAM, A-ugs 64-QAM
This upstream is mapped to physical port 0
Spectrum Group is overridden
US phy MER(SNR)_estimate for good packets - 23.4731 dB
Nominal Input Power Level 3 dBmV, Tx Timing Offset 1645
Ranging Backoff Start 3, Ranging Backoff End 6
US timing offset adjustment type 0, value 0
Ranging Insertion Interval automatic (60 ms)
US throttling off
Tx Backoff Start 3, Tx Backoff End 5
Modulation Profile Group 322
Concatenation is enabled
Fragmentation is enabled
part_id=0x3140, rev_id=0x03, rev2_id=0x00
nb_agc_thr=0x0000, nb_agc_nom=0x0000
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 1
Minislot Size in Symbols = 32
Bandwidth Requests = 0x31
Piggyback Requests = 0x0
Invalid BW Requests= 0x0
Minislots Requested= 0x22C
Minislots Granted  = 0x31
Minislot Size in Bytes = 24
Map Advance (Dynamic) : 2465 usecs
Map Count = 17393154
Remote Map Counts: (none)
UCD Count = 17875
Remote UCD Counts: (none)
SCDMA mode enabled
PHY: us errors 0  us recoveries 0
MAC PHY TSS: tss error start 0  tss error end 0
MAC PHY Status: bcm3140 status 0  lookout status 0
MAP/UCD Replication Instructions:
```

To display the modulation profile of a single logical channel, for default and legacy cable interface line cards, use the **show cable modulation** command:

```
Router# show cable modulation cable 5/0/0 upstream 0

Mod  IUC     Type  Pre Diff FEC  FEC  Scrmb  Max Guard Last Scrmb Pre   Pre   RS
                   len enco T    k    seed   B   time  CW         offst Type
                             BYTE BYTE        siz size  short
381  request qpsk  64  no   0x0  0x10 0x152  0   0     no   yes   400   qpsk0 n
381  initial qpsk  384 no   0x5  0x22 0x152  0   0     no   yes   6     qpsk0 n
381  station qpsk  384 no   0x5  0x22 0x152  0   0     no   yes   6     qpsk0 n
381  short   qpsk  64  no   0x3  0x4C 0x152  12  0     yes  yes   400   qpsk0 n
381  long    qpsk  64  no   0x9  0xE8 0x152  136 0     yes  yes   400   qpsk0 n
381  a-short 64qam 64  no   0x6  0x4C 0x152  6   0     yes  yes   400   qpsk1 n
381  a-long  64qam 64  no   0x9  0xE8 0x152  46  0     yes  yes   400   qpsk1 n
381  a-ugs   64qam 64  no   0x9  0xE8 0x152  35  0     yes  yes   400   qpsk1 n
```

The following example shows a typical output of the **show interface cable** command when multiple logical channels are configured on the indicated cable interface:

```
Router# show interface cable 7/1/0 mac-scheduler 0

     DOCSIS 1.1 MAC scheduler for Cable7/1/0/U0: rate 26880000
     wfq:None
     Queue[Rng Polls] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 1
     Queue[CIR Grants] 0/256, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(7) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(6) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(5) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(4) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(3) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(2) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(1) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 0
     Queue[BE(0) Grants] 0/128, 0 drops, flows 0 fs_demand_ms 0, max 1
     Req Slots 17301958, Req/Data Slots 1440804
```

```
    Init Mtn Slots 498660, Stn Mtn Slots 28134
    Short Grant Slots 0, Long Grant Slots 0
    Adv Phy Short Grant Slots 26, Adv Phy Long Grant Slots 23
    Adv Phy UGS Grant Slots 0
    Awacs Slots 0
    Fragmentation count 0
    Fragmentation test disabled
    Avg upstream channel utilization : 0%
    Avg percent contention slots : 97%
    Avg percent initial ranging slots : 3%
    Avg percent minislots lost on late MAPs : 0%
    Sched Table Rsv-state: Grants 0, Reqpolls 0
    Sched Table Adm-State: Grants 0, Reqpolls 0, Util 0%
    UGS    : 0 SIDs, Reservation-level in bps 0
    UGS-AD : 0 SIDs, Reservation-level in bps 0
    RTPS   : 0 SIDs, Reservation-level in bps 0
    NRTPS  : 0 SIDs, Reservation-level in bps 0
    BE     : 3 SIDs, Reservation-level in bps 0
    MAP TSS: lch_state 11, init_retries 0
             late_initial_maps 0, late_ucd_maps 0
             mac-phy tss errors 0
Router#
```

Configuration Examples for S-CDMA and Logical Channel Support

This section lists the following sample configurations for the S-CDMA and Logical Channel Support feature on a Cisco CMTS router:

Creating Modulation Profiles Examples

This section lists sample configurations for creating the following types of upstream modulation profiles:

Example: DOCSIS 2.0 S-CDMA Modulation Profiles

The following sample configuration shows typical modulation profiles for the DOCSIS 2.0 S-CDMA mode of operation:

- Profile 321 is the default profile for S-CDMA operations that is automatically created on the router for the cable interface line card.
- Profiles 321 through 330 can be used to create S-CDMA modulation profiles.
- Profiles 1 through 400 can be used to create S-CDMA mode modulation profiles, while using the global configuration.

```
cable modulation-profile 321 scdma request 1 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 321 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 321 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 321 scdma a-short 5 131 6 32qam scrambler 152 no-diff m
cable modulation-profile 321 scdma a-long 5 131 0 32qam scrambler 152 no-diff 6m
cable modulation-profile 321 scdma a-ugs 9 232 0 64qam scrambler 152 no-diff 64m
cable modulation-profile 322 scdma request 0 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 322 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 322 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 322 scdma a-short 6 76 6 64qam scrambler 152 no-diff 6m
cable modulation-profile 322 scdma a-long 9 232 0 64qam scrambler 152 no-diff 6m
cable modulation-profile 322 scdma a-ugs 9 232 0 64qam scrambler 152 no-diff 64m
cable modulation-profile 333 scdma request 0 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 333 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
```

```
cable modulation-profile 333 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
--More--
```

Example: Global Modulation Profiles

The following sample configuration shows typical modulation profiles for the global mode of operation. Profiles 1 through 400 can be used to create any modulation profile in global modulation profile mode.

```
cable modulation-profile global-scheme
cable modulation-profile 222 atdma request 0 16 0 22 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma initial 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma station 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 222 atdma a-short 6 76 6 22 64qam scrambler 152 no-dif8
cable modulation-profile 222 atdma a-long 9 232 0 22 64qam scrambler 152 no-dif8
cable modulation-profile 222 atdma a-ugs 9 232 0 22 64qam scrambler 152 no-diff8
cable modulation-profile 223 atdma request 0 16 0 22 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma initial 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma station 5 34 0 48 qpsk scrambler 152 no-diff8
cable modulation-profile 223 atdma a-short 6 76 6 22 64qam scrambler 152 no-dif8
cable modulation-profile 223 atdma a-long 14 220 0 22 64qam scrambler 152 no-di8
cable modulation-profile 223 atdma a-ugs 14 220 0 22 64qam scrambler 152 no-dif8
cable modulation-profile 321 scdma request 1 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 321 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 321 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 321 scdma a-short 5 131 6 32qam scrambler 152 no-diff m
cable modulation-profile 321 scdma a-long 5 131 0 32qam scrambler 152 no-diff 6m
cable modulation-profile 321 scdma a-ugs 9 232 0 64qam scrambler 152 no-diff 64m
cable modulation-profile 322 scdma request 0 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 322 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 322 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 322 scdma a-short 6 76 6 64qam scrambler 152 no-diff 6m
cable modulation-profile 322 scdma a-long 9 232 0 64qam scrambler 152 no-diff 6m
cable modulation-profile 322 scdma a-ugs 9 232 0 64qam scrambler 152 no-diff 64m
cable modulation-profile 333 scdma request 0 16 0 qpsk scrambler 152 no-diff 64m
cable modulation-profile 333 scdma initial 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 333 scdma station 5 34 0 qpsk scrambler 152 no-diff 98m
cable modulation-profile 333 scdma a-short 6 76 6 64qam scrambler 152 no-diff 6m
cable modulation-profile 333 scdma a-long 9 232 0 64qam scrambler 152 no-diff 6m
cable modulation-profile 333 scdma a-ugs 9 232 0 64qam scrambler 152 no-diff 64m
cable modulation-profile 400 scdma-d3 request 0 16 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 initial 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 station 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 short 3 76 12 64qam scrambler 152 no-diffm
cable modulation-profile 400 scdma-d3 long 9 232 0 64qam scrambler 152 no-diff m
cable modulation-profile 400 scdma-d3 a-short 6 76 6 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 a-long 9 232 0 64qam scrambler 152 no-difm
cable modulation-profile 400 scdma-d3 a-ugs 9 232 0 64qam scrambler 152 no-diffm
cable service class 1 name def_sclass
--More--
```

Example: DOCSIS 3.0 S-CDMA Modulation Profiles

The following sample configuration shows typical modulation profiles for the DOCSIS 3.0 S-CDMA mode of operation:

- Profile 381 is the default profile for DOCSIS 3.0 S-CDMA mode operations that is automatically created on the router.
- Profiles 1 through 400 can be used to create DOCSIS 3.0 S-CDMA mode modulation profiles, while using the global configuration.

```
cable modulation-profile 381 scdma-d3 request 0 16 0 64qam scrambler 152 no-difm
cable modulation-profile 381 scdma-d3 initial 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 381 scdma-d3 station 5 34 0 64qam scrambler 152 no-difm
cable modulation-profile 381 scdma-d3 short 3 76 12 64qam scrambler 152 no-diffm
```

```
 cable modulation-profile 381 scdma-d3 long 9 232 0 64qam scrambler 152 no-diff m
 cable modulation-profile 381 scdma-d3 a-short 6 76 6 64qam scrambler 152 no-difm
 cable modulation-profile 381 scdma-d3 a-long 9 232 0 64qam scrambler 152 no-difm
 cable modulation-profile 381 scdma-d3 a-ugs 9 232 0 64qam scrambler 152 no-diffm
 cable modulation-profile 400 scdma-d3 request 0 16 0 64qam scrambler 152 no-difm
 cable modulation-profile 400 scdma-d3 initial 5 34 0 64qam scrambler 152 no-difm
 cable modulation-profile 400 scdma-d3 station 5 34 0 64qam scrambler 152 no-difm
 cable modulation-profile 400 scdma-d3 short 3 76 12 64qam scrambler 152 no-diffm
 cable modulation-profile 400 scdma-d3 long 9 232 0 64qam scrambler 152 no-diff m
 cable modulation-profile 400 scdma-d3 a-short 6 76 6 64qam scrambler 152 no-difm
 cable modulation-profile 400 scdma-d3 a-long 9 232 0 64qam scrambler 152 no-difm
 cable modulation-profile 400 scdma-d3 a-ugs 9 232 0 64qam scrambler 152 no-diffm
  --More--
```

Assigning Modulation Profiles to Upstreams Examples

This section lists sample configurations for assigning the following types of modulation profiles to upstreams:

Example: Assigning DOCSIS 2.0 S-CDMA Modulation Profiles

The following sample configuration shows DOCSIS 2.0 S-CDMA modulation profiles being assigned to the upstreams on two cable interfaces. The default S-CDMA modulation profile (profile 321) is assigned to the upstreams on cable interface 7/1/0, and custom modulation profile 322 is assigned to the upstreams on cable interface 7/1/1.

```
interface Cable7/1/0
 cable init-channel-timeout 160
 no cable mtc-mode
 cable cm-status enable 1-5
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 13
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream ranging-poll interval 25000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 3200000
 cable upstream 0 power-level 3
 cable upstream 0 docsis-mode scdma
 cable upstream 0 spreading-interval 16
 cable upstream 0 codes-per-minislot 4
 cable upstream 0 active-codes 112
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 321
 no cable upstream 0 shutdown
interface Cable7/1/1
 shutdown
 cable cm-status enable 1-5
 no cable packet-cache
 cable downstream channel-id 180
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 1600000
 cable upstream 0 docsis-mode scdma
 cable upstream 0 spreading-interval 16
 cable upstream 0 codes-per-minislot 4
```

```
 cable upstream 0 active-codes 112
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 322
 no cable upstream 3 shutdown
!
```

Example: Assigning Global Modulation Profiles

The following sample configuration shows user-defined DOCSIS 3.0 S-CDMA modulation profiles being assigned to the upstreams on two cable interfaces. Only the first upstream on cable interface 7/1/0 is enabled for A-TDMA mode and assigned an A-TDMA profile. The other two upstreams on cable interface (7/1/1 and 7/1/2) are enabled for custom-defined DOCSIS 3.0 S-CDMA modulation profiles.

```
interface Cable7/1/0
 cable init-channel-timeout 160
 no cable mtc-mode
 cable cm-status enable 1-5
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 13
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream ranging-poll interval 25000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 3200000
 cable upstream 0 ingress-noise-cancellation 112
 cable upstream 0 power-level 3
 cable upstream 0 docsis-mode atdma
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 cable upstream 0 equalization-coefficient
 no cable upstream 0 shutdown
!
interface Cable7/1/1
 shutdown
 cable cm-status enable 1-5
 no cable packet-cache
 cable downstream channel-id 180
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 1600000
 cable upstream 0 docsis-mode tdma
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 frequency 18000000
 cable upstream 1 channel-width 3200000
 cable upstream 1 ingress-noise-cancellation 112
 cable upstream 1 docsis-mode scdma-d3
 cable upstream 1 spreading-interval 16
 cable upstream 1 codes-per-minislot 4
 cable upstream 1 active-codes 64
 cable upstream 1 max-codes-per-subframe 128
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 382
 cable upstream 1 equalization-coefficient
 no cable upstream 1 shutdown
```

```
 cable upstream 2 connector 6
 cable upstream 2 frequency 25000000
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 docsis-mode tdma
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 no cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 frequency 32000000
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 docsis-mode tdma
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 no cable upstream 3 shutdown
!
interface Cable7/1/2
 shutdown
 cable cm-status enable 1-5
 no cable packet-cache
 cable downstream channel-id 181
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 8
 cable upstream 0 frequency 20000000
 cable upstream 0 channel-width 1600000
 cable upstream 0 docsis-mode tdma
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 9
 cable upstream 1 channel-width 1600000
 cable upstream 1 docsis-mode tdma
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 no cable upstream 1 shutdown
 cable upstream 2 connector 10
 cable upstream 2 channel-width 3200000
 cable upstream 2 ingress-noise-cancellation 112
 cable upstream 2 docsis-mode scdma-d3
 cable upstream 2 spreading-interval 16
 cable upstream 2 codes-per-minislot 4
 cable upstream 2 active-codes 64
 cable upstream 2 max-codes-per-subframe 128
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 382
 cable upstream 2 equalization-coefficient
!
```

Example: Assigning DOCSIS 3.0 S-CDMA Modulation Profiles

The following sample configuration shows DOCSIS 3.0 S-CDMA modulation profiles being assigned to the upstreams on two cable interfaces. The default DOCSIS 3.0 S-CDMA modulation profile (profile 381) is assigned to the upstreams on cable interface 7/1/0, and custom modulation profile 382 is assigned to the upstreams on cable interface 7/1/1.

```
interface Cable7/1/0
 cable init-channel-timeout 160
 no cable mtc-mode
 cable cm-status enable 1-5
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 13
```

```
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream ranging-poll interval 25000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 3200000
 cable upstream 0 power-level 3
 cable upstream 0 docsis-mode scdma-d3
 cable upstream 0 spreading-interval 16
 cable upstream 0 codes-per-minislot 4
 cable upstream 0 active-codes 64
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 381
 cable upstream 0 equalization-coefficient
 no cable upstream 0 shutdown
!
interface Cable7/1/1
 shutdown
 cable cm-status enable 1-5
 no cable packet-cache
 cable downstream channel-id 180
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream ranging-poll interval 25000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 3200000
 cable upstream 0 power-level 3
 cable upstream 0 docsis-mode scdma-d3
 cable upstream 0 spreading-interval 16
 cable upstream 0 codes-per-minislot 4
 cable upstream 0 active-codes 64
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 382
 cable upstream 0 equalization-coefficient
 no cable upstream 0 shutdown
```

Example: Creating Logical Channels

The following example shows the configuration of an interface that has two of four physical ports configured to have two logical channels per physical port:

```
interface Cable5/0/0
 no cable packet-cache
 cable downstream channel-id 167
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 max-logical-chans 2
 cable upstream 0 load-balance group 1
 cable upstream 0 0 docsis-mode atdma
 cable upstream 0 0 minislot-size 4
 cable upstream 0 0 power-adjust continue 3
 cable upstream 0 0 range-backoff 3 6
 cable upstream 0 0 modulation-profile 21
 no cable upstream 0 0 shutdown
 cable upstream 0 1 docsis-mode tdma
```

```
 cable upstream 0 1 minislot-size 2
 cable upstream 0 1 power-adjust continue 6
 cable upstream 0 1 range-backoff 3 6
 cable upstream 0 1 modulation-profile 221
 no cable upstream 0 1 shutdown
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 1
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 max-logical-chans 2
 cable upstream 1 0 docsis-mode atdma
 cable upstream 1 0 minislot-size 4
 cable upstream 1 0 range-backoff 3 6
 cable upstream 1 0 modulation-profile 21
 no cable upstream 1 0 shutdown
 cable upstream 1 1 docsis-mode tdma
 cable upstream 1 1 minislot-size 2
 cable upstream 1 1 range-backoff 3 6
 cable upstream 1 1 modulation-profile 221
 cable upstream 1 1 equalization-coefficient
 no cable upstream 1 1 shutdown
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 docsis-mode scdma
 cable upstream 2 frequency 10000000
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 322
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 docsis-mode scdma
 cable upstream 3 spectrum-group 2
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 321
 no cable upstream 3 shutdown
end
```

Additional References

The following sections provide references related to the S-CDMA and Logical Channel Support feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Spectrum Management and Advanced Spectrum Management	Spectrum Management and Advanced Spectrum Management for the Cisco CMTS Routers
Load Balancing and Dynamic Channel Change	Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers

Standards and RFCs

Standards	Title
CM-SP-SECv3.0-I09-090121	Data-over-Cable Service Interface Specifications Security Specification, version 3.0

Standards	Title
CM-SP-CMCIv3.0-I01-080320	Data-over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification, version 3.0
CM-SP-PHYv3.0-I08-090121	Data-over-Cable Service Interface Specifications Physical Layer Specification, version 3.0
CM-SP-MULPIv3.0-I09-090121	Data-over-Cable Service Interface Specifications MAC and Upper Layer Protocols Interface Specification, version 3.0
CM-SP-OSSIv3.0-I08-090121	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 3.0
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

MIBs

MIBs	MIBs Link
• DOCS-BPI-PLUS-MIB • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-CABLE-DEVICE-TRAP-MIB • DOCS-IF-EXT-MIB • IF-MIB • DOCS-IF-MIB (RFC 2670)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

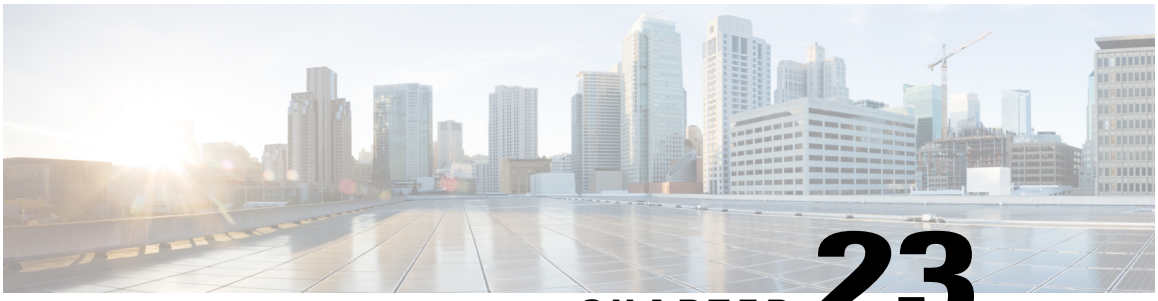
Feature Information for S-CDMA and Logical Channel Support on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 57: Feature Information for S-CDMA and Logical Channel Support on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
S-CDMA and Logical Channel Support on the Cisco CMTS Routers	12.2(33)SCC	This feature was introduced for the Cisco uBR10012 router. The following commands are new or modified: • **cable upstream active-codes** • **cable upstream channel-width** • **cable upstream codes-per-minislot** • **cable upstream docsis-mode** • **cable upstream max-codes-per-subframe** • **cable upstream max-interleave-step** • **cable upstream max-logical-chans** • **cable upstream spreading-interval** • **cable upstream modulation-profile** • **cable upstream modulation-profile global-scheme** • **show controllers cable** • **show interface cable mac-scheduler**
S-CDMA and Logical Channel Support on the Cisco CMTS Routers	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers.



CHAPTER 23

Spectrum Management and Advanced Spectrum Management for the Cisco CMTS

First Published: February 14, 2008

Last Updated: June 20, 2011

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This chapter describes the spectrum management features supported for the Cisco Cable Modem Termination System (CMTS) routers. Spectrum management support is divided into two main groups:

- Guided and scheduled spectrum management features (supported in software)
- Intelligent and advanced spectrum management features (supported in hardware only on specific cable interfaces)

Cisco IOS Release 12.3(13a)BC introduces advanced spectrum management support (software and hardware) for the Cisco uBR10-MC5X20S/U/H broadband processing engine (BPE) in the Cisco uBR10012 universal broadband router.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Spectrum Management and Advanced Spectrum Management

The table below shows the hardware compatibility prerequisites for the spectrum management and advanced management feature supported for the Cisco CMTS routers.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 58: Spectrum Management and Advanced Spectrum Management for the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [40]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [41]

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

40 Cisco uBR3GX60V cable interface line card is compatible with PRE4.

41 Cisco uBR-MC88V cable interface line card is compatible with NPE-G2.

- Guided and scheduled spectrum management features require one of the following Cisco CMTS routers, and one or more of the indicated cable interfaces:

  Cisco uBR7200 series router and one or more of the following cable interfaces:

  - Cisco uBR-MC16U/X cable interface line cards
  - Cisco uBR-MC28U/X cable interface line cards
  - Cisco uBR-MC88V cable interface line cards

  Cisco uBR10012 router and one or more of the following cable interfaces:

  - Cisco uBR10-MC5X20S/U/H cable interface line cards
  - Cisco UBR-MC20X20V cable interface line cards
  - Cisco uBR-MC3GX60V cable interface line cards

- Intelligent and advanced spectrum management (hardware-based, carrier-to-noise ratio [CNR] frequency hopping) requires the following Cisco CMTS routers and one or more of the indicated cable interfaces:

  Cisco uBR7200 series router and one or more of the following cable interfaces:

  - Cisco uBR-MC16U/X cable interface line cards
  - Cisco uBR-MC28U/X cable interface line cards
  - Cisco uBR-MC88V cable interface line cards

  Cisco uBR10012 router and one or more of the following cable interfaces:

  - - Cisco uBR10-MC5X20S/U/H cable interface line cards
    - Cisco UBR-MC20X20V cable interface line cards
    - Cisco uBR-MC3GX60V cable interface line cards

Note You must have Cisco IOS Release 12.3(13a)BC or a later release installed in your router if you are using the Cisco uBR10-MC5X20S/U/H BPE.

- Ensure that your network is designed to support reliable broadband data transmission. At minimum, your network must include:
  - A Dynamic Host Configuration Protocol (DHCP) server to assign IP addresses to cable modems or set-top boxes on the hybrid fiber-coaxial (HFC) network. This can be a server on the WAN side of the Cisco uBR7200 series universal broadband router or a Cisco CMTS router that has been configured to act as the DHCP server.
  - If you are not using cable interface line cards with integrated upconverters, you must install the appropriate IF-to-RF external upconverter between the Cisco CMTS router and the combiner.

    Note The term "combiner" refers to all cables, amplifiers, and taps at the headend or cable distribution center that connect the Cisco CMTS router to the HFC network.

  - Diplex filters installed in the downstream RF path between the cable modems and the cable interface cards in the router. RG-59 headend coaxial cable with the maximum braid available (60 percent + 40 percent braid), double foil, and the correct connector for this cable.
- Avoid frequencies with known ingress problems such as amateur radio bands or short-wave bands.
- Avoid hostile spectrums below 20 MHz.
- When designing your channel plan, allow extra bands for frequency hopping.
- Use the receive power level setting to perform slight equalization adjustments.
- Due to the nature of CATV technology, upstream noise management is a significant issue. We recommend that you follow the rigorous North American plant maintenance procedures documented in the NCTA Supplement on Upstream Transport Issues (available from the National Cable and Telecommunications Association, http://www.ncta.com) to adjust return amplifiers and lasers.

Restrictions for Spectrum Management

This section describes the restrictions for the following spectrum management features:

Shared Spectrum Groups

- Advance spectrum management does not support inter-line-card shared spectrum groups.
- Guided spectrum management does support inter-line-card shared spectrum groups.

Cisco IOS Releases and Cable Interface Line Card Support

The guided and scheduled spectrum management features are available for all currently supported cable interface line cards. These features were released in phases. The table below summarizes the individual features in this basic spectrum management feature set, and the initial Cisco IOS software releases that introduced them.

Table 59: Summary of Guided and Scheduled Spectrum Management Features by Release

Feature	Cisco IOS Release Supported
Frequency Hopping Capabilities, on page 583	12.1(2)EC1, 12.3(4)BC1, and later releases
Dynamic Upstream Modulation (MER [SNR]-Based), on page 584 Frequency Hopping Capabilities, on page 583	12.1(3a)EC1, 12.0(13)SC, 12.3(4)BC1, and later releases
Input Power Levels, on page 587	12.0(6)SC, 12.1(2)EC1, 12.3(4)BC1, and later releases
Advanced Spectrum Management Support Using the Cisco uBR10-MC5X20S/U/H BPE, on page 588	12.3(13a)BC and later releases

The intelligent and advanced spectrum management features were also released in phases. The table below shows the minimum software releases that are needed for these features on the cable interface line cards that support them.

Table 60: Minimum Cisco IOS Releases for Intelligent and Advanced Spectrum Management Support

Cable Interface Line Card	Minimum Cisco IOS Release
Cisco uBR7200 Series Universal Broadband Routers	
Cisco uBR-MC16U/X	12.2(15)CX, 12.3(15)BC2
Cisco uBR-MC28U/X	12.2(15)CX, 12.3(15)BC2
Cisco uBR10012 Universal Broadband Router	
Cisco uBR10-MC5X20S/U/H	12.3(13a)BC

Dynamic Upstream Modulation

- The Cisco CMTS router has one preconfigured (primary) modulation profile that defines a typical profile for quadrature phase-shift keying (QPSK) modulation. To use the Dynamic Upstream Modulation feature, you must create a secondary modulation profile that has a higher modulation scheme than the preconfigured profile. The Three Step Dynamic Modulation feature, supported from Cisco IOS Release

12.2(33)SCB3 onwards, allows you to create and use a third modulation profile. However, the third modulation profile is optional.

- Upstream modulation profiles are assigned to upstream ports and affect all cable modems on those upstream ports.
- Modulation profiles affect the physical layer of the cable network, so only trained technicians who are familiar with the Data-over-Cable Service Interface Specifications (DOCSIS) specifications should create modulation profiles.
- When using the Dynamic Upstream Modulation feature with Voice over IP (VoIP) services, frequent changes to the upstream modulation or channel width could briefly impact the quality of voice calls.

Fixed-Frequency Spectrum Groups with Advanced Spectrum Management

When using cable interface line cards that support advanced spectrum management, do not configure fixed-frequency spectrum groups by specifying a frequency using the **cable spectrum-group frequency** command (for example, **cable spectrum-group 3 frequency 76000000**). If fixed-frequency spectrum groups are desired, configure a band with a starting and ending range, which along with the desired channel width specifies the desired center frequency. In this situation, you must also configure a static channel width so that the Dynamic Upstream Modulation feature does not attempt to hop to a different frequency using a smaller channel width.

For example, to specify a center frequency of 7.6 MHz with a 3.2-MHz channel width, specify a starting frequency of 6.0 MHz (7.6 MHz -1.6 MHz) and an ending frequency of 9.2 MHz (7.6 MHz + 1.6 MHz):

```
Router(config)# cable spectrum-group 15 band 6000000 9200000
Router(config)# interface cable 6/0
Router(config-if)# cable upstream 0 channel-width 3200000 3200000
Router(config-if)# cable upstream 0 spectrum-group 15
```

Note Cisco IOS Release 12.2(8)BC2 does not support spectrum groups with fixed frequencies on the Cisco uBR10012 router.

Limitations on Upstream Modulation Parameters for PacketCable VoIP Calls

We recommend the use of a channel width that is 800 KHz and above while configuring upstreams for PacketCable operations and VoIP calls. (All DOCSIS channel widths and upstream parameter combinations are supported, but not optimum when offering VoIP.)

N+1 Redundancy Support

N+1 redundancy requires the working and protect cable interface line cards to be identical. This ensures that the protect interface supports the same exact configuration as the working interface.

When protecting cards that support intelligent and advanced spectrum management, a switchover preserves the spectrum management configuration, and the protect interface initially uses the same upstream frequency as the working interface. The protect interface does not begin using the advanced spectrum management features until the system stabilizes to avoid any unnecessary frequency hops or channel width changes.

Intelligent and Advanced Spectrum Management Support

- Intelligent and advanced spectrum management is supported on the Cisco uBR10-MC5X20S/U/H cable line interface card in Cisco IOS Release 12.3(13a)BC.
- Cable interfaces use standard DOCSIS, EuroDOCSIS, and the extended Japanese frequency ranges (5 to 55 MHz for upstream interfaces) to support the intelligent and advanced spectrum management features.
- Intelligent and advanced spectrum management features are supported only in the DOCSIS 1.0 and DOCSIS 1.1 Time Division Multiple Access (TDMA) mode of operation. These features cannot be used when a cable interface is operating in the DOCSIS 2.0 mixed, Advanced TDMA (A-TDMA), and Synchronous Code Division Multiple Access (S-CDMA) modes of operation. Similarly, these features are also not available when the cable interface is configured to use multiple logical channels. However, these restrictions do not apply for guided spectrum management.
- Upstream channels must meet the carrier-to-noise plus interference ratio (CNiR [CNR]), and carrier-to-ingress power ratio values given in the DOCSIS specifications. The minimum value for both parameters is 25 dB in the 5 to 65 MHz frequency range.
- The intelligent and advanced spectrum management features do not support inter-line card shared spectrum groups. Spectrum management features require that upstream ports on different line cards have their own RF domain (a unique set of non-overlapping frequencies).
- N+1 redundancy is not supported on any cable interface line card that has defined spectrum groups, which typically is the normal configuration for advanced spectrum management.
- If you are using only one modulation profile and are using a software release prior to Cisco IOS Release 12.2(8)BC2, you need to change the CNR (CNiR) and forward error correction (FEC) threshold parameters from their default values to prevent undesired frequency hopping. This is because in these releases, a frequency hop would occur if just one of the measured values (CNR [CNiR] value, correctable FEC counter, or uncorrectable FEC counter) crossed the configured threshold value. Reducing the CNR (CNiR) threshold or increasing one of the FEC threshold values limits the number of frequency hops.

  This situation no longer occurs in Cisco IOS Release 12.2(8)BC2 and later releases, because a frequency hop can occur only when both the CNR (CNiR) value and one of the FEC counters falls below its threshold value.
- The intelligent and advanced spectrum management feature is activated by assigning spectrum groups on cards with built-in spectrum analyzer.

Information About Spectrum Management

Spectrum management allows a Cisco Cable Modem Termination System (CMTS) to sense upstream plant impairments, report them to a management entity, and automatically correct them where possible. The spectrum management feature performs these functions without reducing throughput or latency and without creating additional packet overhead on the radio frequency (RF) plant.

In particular, because the cable interfaces on the router receive upstream packets, it can directly detect upstream transmission errors. The router can also indirectly monitor the condition of the plant by keeping a record of modem state changes, such as the number and frequency of cable modems that are “flapping” (modems that either miss a station maintenance message or that go offline and then come back online).

Note For more information about the cable modem flapping and how to monitor the cable modem flap list, see the Flap List Troubleshooting for the Cisco CMTS Routers .

Spectrum management can prevent long-term service interruptions caused by upstream noise events in the cable plant. It is also used for fault management and troubleshooting the cable network. When cable modems are detected to go online and offline by flap detectors, the cable operators can look at the flap list and spectrum tables to determine the possible causes.

Because of the nature of cable television (CATV) technology, upstream noise management is a significant issue. Frequency bands must have a sufficient CNR (CNiR) and carrier-to-ingress power ratio to support the transmission of QPSK and quadrature amplitude modulation (QAM) data. The DOCSIS sets the minimum value for both of these ratios to 25 dB in the 5 to 65 MHz frequency range. If the CNR (CNiR) drops below 25 dB on a particular channel due to noise, the cable modem on that channel degrades and can drop off the hybrid fiber-coaxial (HFC) network.

This overview contains the following subsections:

- Spectrum Management Measurements, on page 574—Provides an overview of fundamental concepts and terms that are used in spectrum management.
- Upstream Signal Channel Overview, on page 578—Describes how signals are sent and how changes occur in upstream channels.
- Upstream Segments and Combiner Groups, on page 579—Describes sparse and dense segments and combiner groups.
- Frequency Management Policy, on page 580—Describes the types of noise impairments and how to counteract ingress noise with spectrum groups and frequency hopping.
- Guided and Scheduled Spectrum Management, on page 582—Describes the following guided and scheduled spectrum management features: frequency hopping capabilities, dynamic upstream modulation (signal-to-noise ratio-based), and input power levels.
- Intelligent and Advanced Hardware-Based Spectrum Management, on page 587—Describes spectrum management features that are supported by a number of cable interface line cards that have onboard spectrum management hardware. These features include a real-time spectrum analyzer, CNR-based, proactive frequency hopping, and a more robust dynamic upstream modulation.
- Benefits, on page 589—Describes the spectrum management features provided on the Cisco CMTS router platforms.

Spectrum Management Measurements

Measuring the signal-to-noise ratio (SNR [MER]) and carrier-to-noise ratio (CNR [CNiR]) are the major ways of determining the quality of a downstream or upstream signal. The following sections provide an overview of these two ratios, as well as explaining the differences between them, and some additional values that might be useful:

Signal and Carrier Noise Ratios

Measuring the Modulation Error Ratio (MER [SNR]) and CNR (CNiR) of a downstream or upstream is the first step in determining the quality of the signal, and whether spectrum management needs to be performed to correct any errors. The following are brief descriptions of these two values:

- Modulation Error Ratio (MER [SNR])—This is an estimate of the signal strength on the upstream after ingress noise cancellation is performed. This means that the MER (SNR) takes into account a variety of modulation impairments, including frequency response distortions (such as in-channel amplitude tilt and ripple), group delay, microreflections, and phase noise. The MER (SNR) is a good gauge of the overall end-to-end quality of the cable network, because it includes the impact that the transmitter circuitry, receiver circuitry, and transmission media have on the upstream signal.

  Note The MER (SNR) value was incorrectly calculated in early Cisco IOS software images, reporting a value that was 4 dB larger than expected. This was corrected in Cisco IOS Release 12.1(10)EC1 and Cisco IOS Release 12.2(4)BC1, and later releases. For more information, see Field Notice 44400.

- Carrier-to-Noise Ratio (CNR)—This is an ratio of the measured modulated power, in dB, on the upstream (before ingress noise cancellation is done) that compares the channel power to the noise power.

  The term CNiR is part of the CableLabs nomenclature for the CNR measurement. Therefore these two terms, CNR and CNiR, can be used interchangeably.

  The CNR (CNiR) measurement is usually provided only by an external spectrum analyzer, but the cable interface line cards that support intelligent and advanced hardware spectrum management features also provide CNR (CNiR) measurement.

  Note Starting with Cisco IOS Release 12.2(33)SCF, the CNR (CNiR) measurement is supported for all upstream (US) channels irrespective of whether spectrum management feature is enabled or not for the upstream channels. For all the releases prior to Cisco IOS Release 12.2(33)SCF, the CNR (CNiR) measurement is supported for only those US channels that have spectrum management feature enabled.

  The following two types of CNR (CNiR) measurements are supported on the Cisco CMTS:

  - CNR (CNiR) measured for a particular upstream—This is the overall CNR (CNiR) for all of the cable modems on an upstream, which is determined by measuring the RF power of the upstream receiver at the cable interface. This value is always just a snapshot in time for a particular upstream. The cable interface measures the RF power at a time when no bursts are expected from the cable modems, but it can be skewed by a small number of cable modems that are experiencing or creating signal problems.
  - Per-modem CNR (CNiR)—This is the CNR (CNiR) for a particular cable modem, which is signal strength of the burst transmissions of the modem at the upstream receiver of the cable interface. The per-modem CNR (CNiR) measurement is a very accurate measure of a particular cable modem's signal, but you should not use a single modem's CNR (CNiR) to make assumptions about other cable modems on that upstream or about the upstream itself. However, you can get a good picture of the upstream's signal quality by polling the CNR (CNiR) for a number of cable modems over a representative time period.

Tip Changing the channel width has a direct impact on the CNR (CNiR). Doubling the channel width (for example, from 400 KHz to 800 KHz) decreases the CNR (CNiR) for an upstream by approximately 3 dB. Cutting the channel width in half (for example, from 3.2 MHz to 1.6 MHz) increases the CNR (CNiR) for an upstream by approximately 3 dB.

Differences Between the MER (SNR) and CNR (CNiR) Values

In a perfect network, such as a test lab where the only impairment is additive white Gaussian noise (AWGN), you can expect the CNR (CNiR) and MER (SNR) values to be comparable throughout all of the allowable power levels and frequency ranges. In a live network, however, it is expected that the MER (SNR) value should be a few dB lower than the CNR (CNiR) value, given that the MER (SNR) value takes into account noise impairments and distortions that are not accounted for by the CNR (CNiR) power measurements.

In general, when the CNR (CNiR) value is in the 15 to 25 dB range, you can expect the MER (SNR) value to have a comparable value. The difference between the MER (SNR) and CNR (CNiR) values is expected to be larger when the CNR (CNiR) value falls outside of the 15 to 25 dB range.

The table below provides a comparison between the MER (SNR) and CNR (CNiR) values, listing the major reasons for why the MER (SNR) and CNR (CNiR) values might diverge on an active network that is passing live traffic:

Table 61: Comparison of MER (SNR) and CNR (CNiR) in a DOCSIS Cable Network

Signal-to-Noise (SNR)	Carrier-to-Noise (CNR)
Post-detection measurement of the RF signal.	Pre-detection measurement of the RF signal.
Measurement of the baseband domain.	Measurement of the RF frequency domain.

Signal-to-Noise (SNR)	Carrier-to-Noise (CNR)
Includes the effect of signal distortions and impairments on the signal. These include: • Group delay in the channel such as occurs during operation near the diplexer band edge. • Channel amplitude variation and echoes. • Data collisions. • Microreflections. • Narrow band ingress in the channel. • Non-linearities in the cable plant. • Phase noise. • Poor selection of the preamble. • Poor symbol fidelity in the transmission of a a cable modem, despite a good MER (SNR) value. • Unrecoverable carrier offsets. • Unrecoverable symbol timing offsets.	Measures only the RF modulated carrier power versus noise power.
Provides an indication of overall, end-to-end network quality (what the transmitter, receiver, and transmission media are doing to the signal).	Provides an indication of network performance (what the transmission media or network is doing to the signal).
Average over time with current data traffic patterns, useful for tracking long-term trends in signal quality.	Real-time spectrum analysis.
Reflects the CNR (CNiR) value as part of its value.	Does not reflect the MER (SNR) value as part of its value.
Averaged over 10,000 symbols, and an accurate reading requires that short and long grants are being transferred.	Unaffected by the type of traffic being transmitted.
Does not use packets with uncorrectable FEC errors to determine its value. Bursts of uncorrectable errors, therefore, could result in a deceptively high MER (SNR) value.	Unaffected by uncorrectable FEC packet bursts.
DOCSIS specifications do not define any required MER (SNR) values for upstreams and downstreams.	Minimum downstream CNR of 35 dB in a 6-MHz band (44 dB in DOCSIS 2.0 for 8-MHz band) Minimum upstream CNR (CNiR) of 25 dB.

Additional Measurements

In addition to MER (SNR) and CNR (CNiR) values, you should be aware of and monitor the following indicators of signal quality:

- MER—This is the measure of RF signal quality, in dB, which is equivalent to SNR and similar to CNR (CNiR) under additive white Gaussian noise (AWGN) impairments. However, MER is preferred for data networks, because it also includes additional factors that affect the signal, such as analog-to-digital and digital-to- analog conversions, rounding errors, distortions, and signal impairments such as phase noise, group delay, and jitter. For this reason, the DOCSIS 2.0 RF specification adds a requirement for the minimum MER value for a signal, supplementing the existing CNR (CNiR) minimum requirements.

  A simple formula for calculating the MER value for an upstream is:

  ```
  MER = 20 x log (RMS error magnitude / Average symbol magnitude)
  ```

  You can also calculate the Error Vector Modulation (EVM) to find the equivalent value expressed as a percentage of noise on an upstream:

  ```
  EVM = Average error magnitude / Max symbol magnitude * 100
  ```

  See the DOCSIS 2.0 specification for more complete information on calculating and using the MER value.

- FEC Counters—These are counters that keep track of how many correctable and uncorrectable FEC errors occur on the upstream. The FEC error counters are useful for tracking fast transient errors such as impulse noise that are not usually reflected in MER (SNR) or CNR (CNiR) values.

  A correctable error count of more than 1 percent can be used as a warning sign of possible physical plant or cable modem problems that might be developed. An uncorrectable error count of more than 1 percent can indicate an existing problem that is blocking traffic on the upstream. Cable interface line cards that support the intelligent and advanced spectrum management features can use the FEC counters as one of the indicators to be monitored to determine whether an upstream must change frequencies so as to correct noise problems.

- Microreflections—Additional copies of a signal that arrive at the receiver, usually at different times and attenuated by different amounts, causing the receiver to misidentify the incoming signal's true phase and amplitude. Microreflections typically are caused by impedance mismatches in the physical cable plant, and can indicate either equipment that has been degraded by weather or other causes, or equipment that has not been installed correctly.

Upstream Signal Channel Overview

The upstream channel is characterized by many cable modems transmitting to the CMTS. These signals 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 periodically broadcasts Upstream Channel Descriptor (UCD) messages to all cable modems. The UCD message contains the upstream frequency and transmission parameters associated with an upstream channel. These messages define upstream channel characteristics including the upstream frequencies, symbol rates and modulation schemes, forward error correction (FEC) parameters, and other physical layer values.

Cisco supports all DOCSIS error-correction encoding and modulation types and formats. Upstream signals are demodulated using QPSK or QAM. QPSK carries information in the phase of the signal carrier, whereas QAM uses both phase and amplitude to carry information.

Sending data reliably in the upstream direction is an issue. Because upstream spectrum varies greatly between cable plants, select upstream parameters based on your cable plant's return paths. Select or customize upstream profiles for the maximum trade-off between bandwidth efficiency and upstream channel robustness. For example, QAM-16 requires approximately 7 dB higher CNR (CNiR) to achieve the same bit error rate as QPSK, but it transfers information at twice the rate of QPSK.

Note The above specifications are based on predetermined sets of frequencies that may or may not have an adequate CNR (CNiR) at any given time.

Upstream frequencies can be assigned as follows:

- Fixed—Configuring a spectrum group disables the fixed upstream frequency setting.
- Single subband—The CMTS administrator can define a center frequency and symbol rate such that the boundaries of the upstream carrier stay within the subband. The frequency and symbol rate can change within the boundary in response to noisy line conditions, based on the defined upstream parameters.
- Multiple subbands—The data carrier can remain in a particular subband for a duration of time and then hop to another subband based on the defined upstream parameters.

Tip Measurement of noise power levels with a spectrum analyzer should be part of the procedure in initially selecting and setting up frequency allocations. We recommend having fixed frequency settings during early deployment, at least until amplifier cascade adjustments or plant repair have become infrequent enough that they no longer significantly affect the nodes connected to the upstream port.

Upstream Frequency Changes

As stated in the DOCSIS radio frequency interface (RFI) specification, RF channel migration or upstream frequency change occurs when a change in the UCD message is broadcast to all cable interfaces.

The speed of channel migration via the UCD message is typically less than 20 milliseconds (ms). During this time, upstream transmission is interrupted until the cable interface transmitter adjusts to its new frequency. Data is stored in the cable interface buffers during this time and is sent when the frequency hop is complete.

Station maintenance intervals are used to perform per modem keepalive polling. The CMTS polls each cable modem at least once every 30 seconds, with the default being once every 20 seconds. When ingress noise causes loss of keepalive messages from a configurable percentage of all cable interfaces, resulting in missed polls, a new frequency is selected from the allocation table and a UCD update is performed. The migration time is 2 msec for any upstream UCD update. After the UCD is updated, the hop occurs. The system must wait until a hop threshold time interval has elapsed before it can change the UCD a second time.

Upstream Segments and Combiner Groups

The Cisco routers divide a cable plant into downstream channels. Downstream channels contain upstream segments. Each upstream segment typically serves more than one fiber node. Upstream segments can be defined as one of the following:

- Sparse segment—Containing one upstream channel per upstream segment.

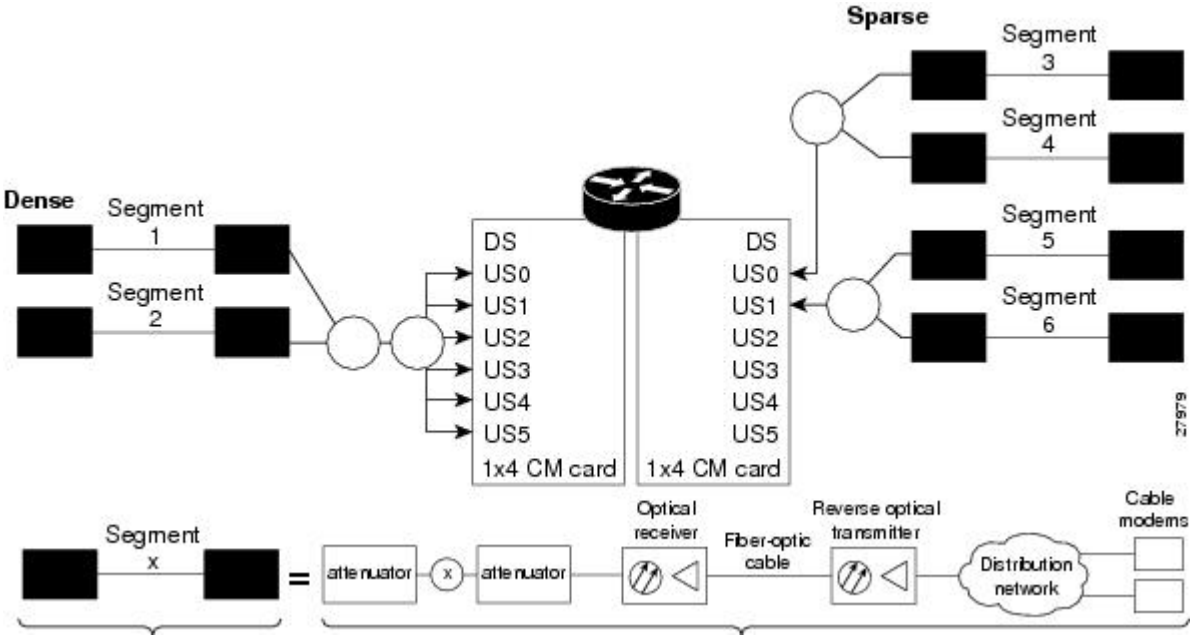
- Dense segment—Containing multiple upstream channels per upstream segment; frequencies must be different.

Note A cable interface line card can support sparse or dense segments, or both.

Defining sparse segments allows the cable operator to share upstream bandwidth among fiber nodes with fewer subscribers. Defining dense segments allows the cable operator to provide larger upstream bandwidth to fiber nodes with many subscribers.

The figure below illustrates sparse versus dense segments.

Figure 8: Sparse Versus Dense Segment Illustrations



As shown in the figure above, the downstream segment can contain multiple upstream segments. Two fiber nodes can be in one downstream segment but in different upstream segments.

The return path of several fiber nodes can be combined at a single point to form a single RF frequency domain called a combiner group. The CMTS software allows a frequency hop table called a spectrum group to be associated with a combiner group.

Note A combiner group refers to an RF topology point. A spectrum group refers to the frequency hop table associated with a combiner group.

Frequency Management Policy

Spectrum management applies a common frequency-management policy to a set of upstream ports to ensure that data is delivered reliably over the cable plant. Cable plant operators must make noise measurements and

determine the cable plant's spectrum management policy. Different modulation schemes, upstream frequency techniques, and symbol rates are used based on the cable plant characteristics and the cable interface line card in the chassis.

See the following sections for more information about these topics:

Noise Impairments

Upstream noise impairments such as signal degradation on cable networks can negatively affect service to subscribers. Two-way digital data signals are more susceptible than one-way signals to stresses in the condition of the HFC network. Degradation in video signal quality might not be noticeable in one-way cable TV service, but when two-way digital signals share the network with video signals, digital signals can be hampered by:

- Impulse and electrical signal ingress—Noise can enter the network from electrical sources within a residence or from high-voltage lines that run near cable television cabling. Two types of ingress noise include broadband and narrowband. Broadband noise is generally of lower frequency (below 10 MHz) and results in harmonic rolloff. Narrowband noise is a more significant interference source. Cable equipment and infrastructure often pick up noise from amateur radio transmissions, citizen band radios, or high-power shortwave broadcast signals. Implement a signal leakage maintenance program to locate and repair areas of signal ingress.
- Amplifier noise—Amplifiers add noise to the HFC network that typically goes unnoticed in video signals, but degrades digital data signals if amplifiers are improperly configured. The larger the network, the higher the probability of amplifier noise affecting signals.
- Noise funneling—The upstream data path to the headend is susceptible to interference from the entire network. All upstream noise ultimately ends up at the headend because the cumulative nature of noise becomes concentrated at the headend. As a network serviced by a single RF receiver increases in size, the probability of noise funneling also increases.
- Variable transmit levels—Temperature affects signal loss over coaxial cable. This can cause variations of 6 to 10 dB per year.
- Clipping—The lasers in fiber-optic transmitters can stop transmitting light when input levels are excessive. Excessive input levels introduce bit errors in both the upstream and downstream transmissions. If a laser is overdriven as briefly as a fraction of a second, clipping can occur.

To adjust your return amplifiers and lasers, follow rigorous plant maintenance procedures documented in the NTSC Supplement on Upstream Transport Issues or appropriate cable plant standard.

Spectrum Groups and Frequency Hopping

We recommend that CMTS administrators configure upstream frequency hopping to counteract long-term, narrowband noise. Cisco CMTS routers support a combination of guided frequency hopping and time-scheduled frequency hopping.

The frequency hop to proactively avoid noise ingress is sometimes called frequency agility. Frequency agility is configured and activated using spectrum groups. Spectrum management supports the creation of a number of cable spectrum groups, allowing multiple upstream ports in a single spectrum group. Each spectrum group defines the table of frequencies to be used in a specific frequency plan. Upstream frequencies can be a fixed single frequency, a single continuous range of frequencies (band), or multiple ranges (or bands) of frequencies.

The cable interface does not operate until you assign a frequency to the upstream, which can be done either by configuring and assigning a spectrum group or assigning a fixed frequency. The spectrum group takes

precedence, so if you configure both a spectrum group and a fixed frequency on an upstream, the spectrum group overrides the fixed upstream frequency setting.

From the interface point of view, a spectrum group also represents the set of upstreams connected to the same group of fiber nodes. The spectrum manager software in Cisco routers examines all the RF parameters that have been configured on an upstream to determine whether the upstream frequencies need to be managed together. For example, if you configure a spectrum group with several fixed frequencies, but those frequencies are all within the configured channel width, the spectrum manager software combines the frequencies into a single band.

The upstream ports use the spectrum group to determine which frequencies are available if frequency hopping is needed to deal with noise or other path impairments. The types of frequency hopping techniques are guided, time-scheduled, and combined guided and time-scheduled. See the Frequency Hopping Capabilities, on page 583 for more information on the types of frequency hopping techniques.

Note When each upstream port has its own RF domain, the group is called a nonshared spectrum group. When multiple upstream ports share the same RF domain, the group is called a shared spectrum group.

Guidelines for Spectrum Management

In general, when defining your spectrum, use the following guidelines:

- Avoid frequencies with known ingress problems, such as amateur radio bands or short-wave bands.
- Avoid a hostile spectrum below 20 MHz.
- Allow extra bands for frequency hopping.
- Take the possible channel widths into account when creating frequency bands. The range of frequencies being used must be able to hop between at least two different frequencies when using the channel width that is configured on the upstream.
- Place upstream ports in the same combiner group in a shared spectrum group.
- Use the receive power level setting to perform slight equalization adjustments.
- If you combine multiple upstream ports to provide increased bandwidth, you must avoid overlapping frequency bands. Each port should be using a discrete band of frequencies that does not overlap the bands being used by other ports in the group. We recommend adding at least 20 KHz between the ending frequency of one band and the starting frequency of the next band, to ensure that the bands do not overlap.

Guided and Scheduled Spectrum Management

Guided and scheduled spectrum management constitutes a set of basic features for all currently supported cable interface line cards. These features are considered basic because they are available for all cable interfaces, and constitute the elementary, cornerstone features upon which the intelligent and advanced spectrum management features are built.

See the following sections for more information about each feature:

Frequency Hopping Capabilities

Noise in the upstream transmission line, that is from the consumer to the service provider, can degrade data transmission from the subscriber's home. If the noise impairment is of substantial duration, it may cause the cable modem to temporarily lose communication with the headend facility. As a contingency plan, the multiple service operators (MSOs) can reserve multiple channels or upstream frequencies for their subscribers. If one channel suffers too much interference, the CMTS requests that the cable modems "hop" to another channel.

To provide frequency hopping capability, Cisco CMTS routers contain a spectrum manager that continuously monitors the noise in unused upstream channels. If the CNR (CNiR) reaches an unacceptable level on a particular channel, the spectrum manager automatically assigns a new upstream channel to the cable modem using that channel.

Cisco CMTS routers support the following techniques for upstream frequency hopping when the frequency band in use is not clean:

- Guided frequency hopping—In guided frequency hopping (also known as blind hopping), the spectrum manager automatically assigns a new upstream channel frequency when a configurable threshold of station maintenance (keepalive) messages fails. Failed station maintenance messages represent an impairment of the upstream channel due to noise, plant, or equipment failure. Explicit frequency subbands and associated input power levels are assigned in a spectrum group in guided frequency hopping.
- Time-scheduled frequency hopping—Frequency reassignment is scheduled by the time of day or by a specific day of the week.
- Combined guided and time-scheduled frequency hopping.

Note Frequency hopping is not effective against broadband noise phenomena such as impulse noise.

Time-scheduled and guided hopping techniques are independent concepts:

- The spectrum is controlled by a script, not a frequency table.
- The available spectrum is time-scheduled as an option.
- A guided hopping frequency is selected from the available spectrum at the current time.

You can configure and activate frequency hopping by using spectrum groups. You can create up to 40 cable spectrum groups, each containing multiple upstream ports. The configured channel width is used for each upstream frequency.

After you have created one or more spectrum groups for your cable network, you can add characteristics to them, providing you with more definitive control over frequency usage and frequency hopping.

You can configure hopping thresholds. For example, the frequency hop threshold percentage method prevents a single failing cable modem from affecting service to other working cable modems. As long as a high enough threshold is configured, the system does not hop endlessly due to a single cable modem failing to respond to 90 percent of its station maintenance (keepalive) messages.

You can also configure the minimum period between frequency hops, with a default setting of 30 seconds. If the destination channel is expected to be impaired, you can reduce the minimum period between frequency hops to a small value, such as 10 seconds. This allows the frequency hop to continue more rapidly until a clear channel is found. If excessive frequency hop is an issue, you can increase the minimum period between hops.

To configure different techniques of frequency hopping, see the Creating and Configuring Spectrum Groups, on page 592.

Note Spectrum management is not supported for one-way (telco return) cable modems, because spectrum management capabilities focus on the upstream path over an HFC network.

Note After the spectrum-band is changed, the spectrum management does not rearrange the frequency for each US channel if the previous frequency belongs to the range of new spectrum-band, which means that the US frequency will not be changed; if the previous frequceny is out of range of new spectrum-band, those US channels will not get frequencies.

Guided Frequency Hopping

Guided frequency hopping is called “guided” because the frequency hopping uses the frequencies that are specified in the spectrum group, which can be either a set of discrete frequencies or a band. The cable interface line cards that support guided frequency hopping do not have a “look-ahead” mechanism that would allow them to determine the quality of the new frequency or band ahead of time, which is why previous documents referred to this as blind hopping. Because of this, though, the cable interface does not need to perform any search on the new potential frequencies, so the switching time between frequencies is only approximately 20 milliseconds.

You can specify some rules the system uses when hopping to another frequency when the frequency band in use is not clean. You can assign explicit frequency subbands and associated input power levels in a spectrum group. All cable modems then on the upstream port migrate to the next frequency with an assigned input power level. The number of lost station management messages exceeding a configured threshold can initiate an upstream channel frequency reassignment. For example, you can specify a frequency hop based on lost station management messages that exceed a threshold. The default threshold may be 10 to 20 percent depending on the Cisco IOS release. The frequency change occurs rapidly without data loss and with minimal latency.

Take care to reduce the spectrum allocation when it is used with small channel widths. Otherwise, there will be a large number of upstream channel slots. For example, if the allocation is from 20.0 to 28.0 MHz and an upstream port has its channel width set to 0.2 MHz, there are 40 possible slots for that channel width. Guided frequency hopping can require a long time to find the clean slot, because it tries each available slot, one at a time, for several seconds during each try.

Time-Scheduled Frequency Hopping

You can specify upstream channel frequency reassignment based on a configured time of every day or of a specific day of the week. If your cable plant has an upstream noise characteristic on a weekly cycle, use time-scheduled spectrum allocation. With a time-scheduled policy, a single frequency becomes valid at any given time.

Dynamic Upstream Modulation (MER [SNR]-Based)

The basic Dynamic Upstream Modulation feature is supported on all Cisco cable interface line cards beginning with Cisco IOS Release 12.1(3a)EC1, Cisco IOS Release 12.2(4)BC1b, Cisco IOS Release 12.2(33)SCC and later releases.

This section describes the operation of this feature, which is based on evaluating the MER (SNR) of an upstream.

Note A more advanced version of dynamic upstream modulation, which uses the carrier-to-noise ratio (CNR [CNiR]), is supported on the cards that support intelligent and advanced spectrum management.

Feature Overview

Cisco cable interface line cards monitor the MER (SNR) values and the forward error correction (FEC) counters in the active return path of each upstream port. The Dynamic Upstream Modulation feature determines whether upstream channel signal quality can support the modulation scheme configured, and adjusts to the most robust modulation scheme when necessary. When return path conditions improve, this feature returns the upstream channel to the higher modulation scheme that includes the modulation profile.

A modulation profile is a collection of burst profiles that are sent out in a UCD message to configure modem transmit parameters for the upstream. The Dynamic Upstream Modulation feature adjusts the modulation profiles of an upstream channel based on upstream signal quality.

The Dynamic Upstream Modulation feature is configured on interfaces with fixed upstream frequencies or on interfaces with assigned spectrum groups.

The following examples show two different configurations of the Dynamic Upstream Modulation feature, using two and three modulation profiles.

Example Showing Dynamic Upstream Modulation Using Two Modulation Profiles

You can configure the Dynamic Upstream Modulation feature on the Cisco CMTS router using the following primary and secondary modulation profiles:

- The primary modulation profile uses 64-QAM or 16-QAM, which is a more bandwidth-efficient modulation scheme and has a higher throughput than a QPSK profile.
- The secondary modulation profile uses QPSK, which uses a more robust modulation scheme, but is not bandwidth-efficient.

We recommend that the primary profile use 64-QAM or 16-QAM modulation and the secondary use QPSK. However, this is optional as both modulation profiles can either be QPSK or QAM. It is not mandatory for one profile to be QAM and the other QPSK, but modulation profile switchover is tied to the QAM and QPSK thresholds.

Example Showing Dynamic Upstream Modulation Using Three Modulation Profiles

You can configure the Dynamic Upstream Modulation feature on the Cisco CMTS router using the following primary, secondary, and tertiary modulation profiles:

- The primary modulation profile uses 64-QAM, which is a more bandwidth-efficient modulation scheme and has a higher throughput than a 16-QAM profile.
- The secondary modulation profile uses 16-QAM, which is a more bandwidth-efficient modulation scheme and has a higher throughput than a QPSK profile.
- The tertiary modulation profile uses QPSK, which uses a more robust modulation scheme, but is not bandwidth-efficient.

We recommend that the primary profile use 64-QAM modulation, the secondary profile use 16-QAM, and the tertiary profile uses QPSK. However, this is optional as the modulation profiles can either be QPSK or QAM. It is not mandatory that one is QPSK and the other two are QAM, but modulation profile switchover is tied to the QAM and QPSK thresholds.

Note Support for Three Step Dynamic Modulation is available from Cisco IOS Release 12.2(33)SCB3 onwards.

Tip Cisco IOS Release 12.2(15)BC2 introduced a series of robust predefined modulation profiles that can also be used with the Dynamic Upstream Modulation feature. See the description of the **cable modulation-profile** command in the Cisco IOS CMTS Command Reference for more information.

Criteria for Switching Modulation Profiles

The Dynamic Upstream Modulation feature uses the following criteria to determine whether it should switch from the primary modulation profile (the more bandwidth-efficient, but less robust profile) to the secondary modulation profile (more robust, but less bandwidth-efficient profile) or to the (optional) tertiary modulation profile (most robust, but less bandwidth-efficient profile):

The modulation switch from the primary profile (high performance) to the secondary profile (mid-level performance) uses the following criteria:

- The upstream MER (SNR) is less than MER (SNR) threshold one and the percentage of correctable FEC (cFEC) errors is greater than or equal to the correctable FEC error threshold or the percentage of uncorrectable FEC (uFEC) errors is greater than or equal to the uncorrectable FEC error threshold.

Before switching back to the primary profile from the secondary profile, the following criteria must be satisfied:

- The upstream MER (SNR) is greater than or equal to the sum of MER (SNR) threshold one and the hysteresis value and the percentage of correctable FEC errors is less than or equal to the correctable FEC error threshold and the percentage of uncorrectable FEC errors is less than or equal to the uncorrectable FEC error threshold and the hop period equals to the default value of 15 seconds.

The modulation switch from the secondary profile (mid-level performance) to the tertiary profile (most robust) uses the following criteria:

- The upstream MER (SNR) is less than MER (SNR) threshold two and the percentage of correctable FEC (cFEC) errors is greater than or equal to the correctable FEC error threshold or the percentage of uncorrectable FEC (uFEC) errors is greater than or equal to the uncorrectable FEC error threshold.

Before switching back to the secondary profile from the tertiary profile, the following criteria must be satisfied:

- The upstream MER (SNR) is greater than or equal to the sum of MER (SNR) threshold two and the hysteresis value and the percentage of correctable FEC errors is less than or equal to the correctable FEC error threshold and the percentage of uncorrectable FEC errors is less than or equal to the uncorrectable FEC error threshold.

The modulation switch from the primary profile to the tertiary profile uses the following criteria:

- The upstream MER (SNR) is less than MER (SNR) threshold two and the percentage of correctable FEC (cFEC) errors is greater than or equal to the correctable FEC error threshold or the percentage of uncorrectable FEC (uFEC) errors is greater than or equal to the uncorrectable FEC error threshold.

Before switching back to the primary profile from the tertiary profile, the following criteria must be satisfied:

- The modulation switch from the tertiary profile to the primary profile is a two-step process:

  1. The modulation switch happens from tertiary profile to the primary profile, when the upstream MER (SNR) is greater than or equal to the sum of MER (SNR) threshold one and the hysteresis value.
  2. After a 15-second (non-configurable) delay, the modulation switch occurs from secondary profile to the primary profile, when the upstream MER (SNR) remains greater than or equal to the sum of MER (SNR) threshold one and the hysteresis value.

If the only problem is that the upstream is experiencing a large number of uncorrectable errors, then a situation could occur where the router continues to switch back and forth between profiles. The uncorrectable errors occur with the primary profile, so the router switches to the secondary profile. The secondary profile does not experience any problems, so the router switches back to the primary profile. But the uncorrectable errors reoccur and the router switches back to the secondary profile, and this cycle continues indefinitely.

To avoid this problem, make sure that the cable plant is capable of supporting the modulation scheme being used in the primary profile (for example, 64-QAM). If you cannot guarantee successful operation on an upstream using this modulation scheme, then you should select a primary profile that uses a more bandwidth-efficient set of burst parameters (such as QPSK). The Cisco IOS software includes predefined modulation profiles that can be used for the primary, secondary, and tertiary profiles.

Input Power Levels

Upstream input power level modifications were made in Cisco IOS Releases 12.0(6)SC, 12.1(1), 12.1(1)T, 12.1(2)EC1, and 12.2(4)BC1b.

The input power level, *power-level-dBmV*, is an option in the **cable spectrum-group** command. The option allows you to specify the expected upstream 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 Configuring and Assigning Spectrum Groups, on page 603.

Intelligent and Advanced Hardware-Based Spectrum Management

Several cable interface line cards include hardware-based spectrum management features that provide enhancements to the basic features supported by the other Cisco cable interface line cards.

Intelligent Spectrum Management Enhancements

The following features are part of the intelligent spectrum management feature set:

- Integrates a DOCSIS cable interface line card with an onboard spectrum analyzer that continuously analyzes the upstream spectrum quality in the DOCSIS frequency range of 5 to 42 MHz.
- Includes hardware-assisted frequency hopping, providing for more intelligent and faster frequency selection than software-only solutions.
- Reduces the response time to ingress noise that could cause modems to drop offline.
- Eliminates blind frequency hopping by initiating frequency hops to known clean channels.
- Improves frequency agility to help eliminate dropped packets and thereby maintain full upstream data rates.
- Supports frequency agility in dense-mode combining environments across a shared spectrum.
- Restricts frequency hopping to a set of discrete fixed frequencies or to a range of frequencies, as desired.
- Allows frequency hop conditions to be customized for specific plant environments and requirements.
- Optionally schedules frequency hops to take advantage of known usage patterns or plant conditions.
- Optionally dynamically reduces channel width to allow cable modems to remain online, even in noisy upstream conditions.

Advanced Spectrum Management Support Using the Cisco uBR10-MC5X20S/U/H BPE

The advanced spectrum management features were introduced on the Cisco uBR10-MC5X20S/U/H BPE as a software-only upgrade. These enhancements are supported on additional line cards on the Cisco IOS Releases that are shown in Table 60: Minimum Cisco IOS Releases for Intelligent and Advanced Spectrum Management Support, on page 571.

The following additional features are part of the advanced spectrum management feature set:

- Supports proactive channel management, to avoid the impacts of ingress and keep subscribers online and connected.
- Offers flexible configuration choices, allowing users to determine the priority of the actions to be taken when ingress noise on the upstream exceeds the allowable thresholds. The configurable actions are frequency hopping, switching the modulation profile, and reducing the channel width.
- Performs carrier-noise ratio (CNR [CNiR]) calculations in real time on a per-interface and a per-modem basis.

Note In Cisco IOS Release 12.3(13a)BC and later Cisco IOS 12.3 BC releases, the CNR (CNiR) value is before the Ingress Noise Cancellation, while the MER (SNR) value is after the Ingress Noise Cancellation. For this reason, the CNR (CNiR) and MER (SNR) values might not exactly match for any particular period.

- Determines when to modify the frequency, channel width, or modulation profile, based on the CNR (CNiR) and MER (SNR) calculations in the active channel and the number of correctable FEC errors and uncorrectable FEC errors. Frequency hopping, channel width change, or profile change occurs in the following circumstances:

- The CNR (CNiR) and MER (SNR) values fall below the user-defined threshold value for the primary modulation profile and the correctable FEC error value or the uncorrectable FEC error exceeds its user-defined threshold.

This logic can be expressed as the following formula:

```
[(CNR <= threshold) AND (MER(SNR) <= threshold)] AND
[ (correctable FEC >= threshold) OR (uncorrectable FEC >= threshold)]
```

This approach helps avoid unneeded channel changes due to transient noise problems that do not actually cause any errors in the data stream. The channel changes only when the noise affects both the CNR (CNiR) and MER (SNR) of the upstream and generates an unacceptable number of FEC errors in the data. If you want channel changes to occur only in response to the CNR (CNiR), you must set the MER (SNR) threshold and the FEC error threshold values to zero.

Separate CNR (CNiR) threshold values are configured for the primary and secondary modulation profiles. When the upstream has moved to the secondary modulation profile, further frequency hopping or channel width changes occur only when the CNR (CNiR) and the MER (SNR) values fall below the user-defined threshold value for the secondary profile.

Note Previously, channel hopping occurred when the number of missed station maintenance polls exceeded a user-defined threshold or the MER (SNR) exceeded a certain threshold.

- Enhances the Dynamic Upstream Modulation feature for the Cisco uBR10-MC5X20S/U/H BPE. This feature supports dynamic modulation using two upstream profiles. The primary profile (typically using QAM-16 “mix” modulation) remains in effect at low noise conditions, but if upstream conditions worsen, the cable modems switch to the secondary profile (typically using QPSK modulation) to avoid going offline. When the noise conditions improve, the modems are moved back to the primary profile.
- Provides an SNMP interface so that a network management workstation or other graphical tool can obtain spectrum information for either a particular cable modem or for an entire upstream. The frequency resolution can be as fine as 10 KHz for Cisco uBR10-MC5X20S/U cable interface line card and 20 KHz for Cisco uBR-MC28U and Cisco uBR10-MC5X20H cable interface line cards.

Note The CISCO-CABLE-SPECTRUM MIB has been enhanced to provide this support.

Benefits

The spectrum management features provided on the Cisco CMTS router platforms provide several key system benefits:

- Improves response time to ingress noise impairments that appear in the upstream return path.
- Boosts the percentage of modems online.
- Mitigates the impact of ingress to subscriber services.
- Saves time and effort by MSO staff when troubleshooting minor plant outages.
- Increases cable plant reliability.

- Maximizes spectrum utilization.

Guided and Scheduled Spectrum Management Benefits

The following summarizes the specific benefits of the guided and scheduled spectrum management features that are supported for all Cisco CMTS router platforms.

Input Power Levels

Allows the cable plant operator to perform minor power level equalization as a function of frequency.

Frequency Hopping Capabilities

Proactively countermeasures upstream noise impairments by assigning a new upstream channel to the cable modem. MSOs can take advantage of this feature especially when they have less than an optimal carrier-to-noise ratio in the upstream frequencies or when their cable plants exhibit random bursts of ingress noise that affect reliability.

Dynamic Upstream Modulation

- Reduces the risk associated with transitioning to QAM-16 modulation in the return path and provides assurance that subscribers remain online and connected during return path impairments.
- Checks that the active upstream signal quality can support the configured modulation scheme and proactively adjusts to the more robust modulation scheme when necessary.
- Eliminates the necessity to hop channels for cable modems to stay online by automatically switching from the primary modulation profile to the secondary modulation profile.

Intelligent and Advanced Spectrum Management Benefits

The following summarizes the specific benefits of the advanced spectrum management features that are supported on Cisco CMTS routers using supported cable interface line cards.

Dynamic Channel Width Change

- Improves the DOCSIS upstream channel availability by finding the maximum possible channel width for an upstream when noise conditions make the current channel width unusable.
- Provides the maximum RF spectrum utilization efficiency for current plant conditions.
- Customizable range of channel widths that can be used to respond to noise problems.

Intelligent Frequency Hopping

- Proactively changes upstream frequency for an interface before noise conditions become severe enough to force cable modems offline.
- Dedicated hardware intelligent frequency hopping performs “look-ahead” to choose new upstream frequency to find a stable channel.
- Flexible priority configuration allows hopping decision criteria to be tailored to the individual cable plant environment.

- Improves responsiveness to ingress impairments, by matching the hopping decision criteria to the fluctuating plant conditions.
- Pinpoints CNR (CNiR) variations with per-modem accuracy to isolate problematic cable modems.
- Sustains or even improves subscriber online percentages through user-programmable proactive channel management techniques.

Dynamic Upstream Modulation

- Reduces the risk associated with switching between QPSK and QAM-16 modulation in the upstream to respond to ingress noise, so that subscribers remain online and connected.
- Checks the current upstream signal to ensure that it can support the configured modulation scheme, and proactively adjusts to the secondary more robust modulation scheme when necessary.
- Improves DOCSIS upstream channel availability and provides maximum RF spectrum utilization efficiency.
- Eliminates unnecessary frequency hopping by switching modulation profiles to one that allows cable modems to remain online while using the currently assigned upstream.
- Provides assurance that subscribers remain online and connected during periods of return path impairments.

SNMP Interface

- Provides a way to remotely obtain the current status of noise on an upstream. This information can then be inserted into third-party or custom reporting and graphing applications.
- Provides visibility to ingress and impulse noise under the carrier frequency on a per-port basis.
- Provides an easy-to-use, distributed method to remotely gather real-time display of the DOCSIS upstream spectrum for individual cable modems and set-top boxes (STBs).
- Reduces the reliance on costly spectrum analyzers at every headend or hub.
- Quickly provides spectrum views through an intuitive interface, without the complicated setup time of a spectrum analyzer.
- Allows the technician to troubleshoot the network remotely, as opposed to having to be physically present to connect and use a spectrum analyzer.

Default Hop Priority

For Intelligent and Advanced Spectrum Management feature, the default hop priority is as given below:

- Frequency, modulation, and channel width (when using spectrum groups on spectrum cards).
- Modulation, guided frequency hop, and channel width (when using analyzer cards with spectrum groups).
- Modulation only (when not using spectrum groups [fixed frequency]).

How to Configure Spectrum Management

This section describes the configuration tasks that are most commonly performed when using the spectrum management features on the Cisco CMTS platforms. See the following sections for the configuration tasks that are appropriate for your platform and cable interface line cards.

Guided and Scheduled Spectrum Management Configuration Tasks

The following tasks configure the guided and scheduled spectrum management features that are supported on all Cisco CMTS platforms:

Creating and Configuring Spectrum Groups

A spectrum group defines the frequencies that an upstream is allowed to use when frequency hopping is done, as well as other parameters that control the frequency hops. When creating and configuring spectrum groups, you can specify the following parameters:

- Frequencies that are assigned to the group. The cable interface uses these frequencies to determine what frequencies are available to use when frequency hopping is needed. You can specify either a list of fixed frequencies or a band of frequencies, or both. The Cisco CMTS uses the following rules when adding frequencies to a spectrum group:
  - When specifying a fixed frequency, the Cisco CMTS assumes it is a center frequency with a 6.4-MHz channel width to allow that frequency to operate at all possible channel widths. For example, specifying a frequency of 17,700,000 Hz is equivalent to specifying a frequency band from 14,500,000 Hz to 20,900,000 Hz (a band that is 6.4 MHz wide).
  - If you configure multiple fixed frequencies or bands of frequencies that overlap, the spectrum group combines them into one band. For example, if you specify a fixed frequency of 17,700,000 Hz and a band from 15,800,000 Hz to 25,200,000 Hz, the spectrum group is configured with one band from 14,500,000 Hz to 25,200,00 Hz.
  - If you want more control over a spectrum group's frequencies, configure bands of frequencies with the same width as the desired channel width. For example, if you want to use a center frequency of 17,700,000 Hz with a 3.2-MHz channel width, specify a band that ranges from 16,100,000 Hz to 19,300,000 Hz. To ensure you configure non-overlapping bands, separate the bands by a minimum of 20 KHz.
- Upstream input power level—(Optional) Power level, in dBmV, that the upstream should use when hopping to a new frequency. (Some cable plants might want to change only the input power level, and not the frequency, on a daily time schedule.)
- Hop threshold—(Optional) Percentage of cable modems that start missing station maintenance messages before a frequency hop can occur. Configure the hop threshold percentage as needed to prevent a single failing cable interface from affecting service to other good cable interfaces. This ensures that the system does not hop endlessly because one cable modem is generating 90 percent of the errors and 90 percent of the traffic.
- Hop period—(Optional) Minimum time period that must elapse between frequency hops. This allows you to specify a time period long enough to allow an upstream to stabilize before another frequency hop can be performed.

- Scheduled hop time—(Optional) Time of day at which a frequency hop should be scheduled.
- Shared—(Optional) Specifies that all the upstream ports using a spectrum group should use a unique frequency.

Tip Before adding a list of upstream frequencies (or frequency hop tables), start by determining which upstream ports are assigned to a combiner group. Refer to the Example: Determining the Upstream Ports Assigned to a Combiner Group, on page 623 for an example.

Restriction

- The Cisco uBR10012 universal broadband router does not support spectrum management groups with fixed frequencies for the Cisco MC5X20S/U/H. The Cisco uBR7246VXR universal broadband router does not support spectrum groups with fixed frequencies for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X line cards.
- The Cisco uBR10012 universal broadband router does not support inter-line card shared spectrum groups for the Cisco MC5X20S/U/H. The Cisco uBR7246VXR universal broadband router does not support inter-line card shared spectrum groups for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X line cards.

To create and configure a spectrum group, use the following procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable spectrum-group** *group-number* [**time** *day hh:mm:ss*] **frequency** *up-freq-Hz* [*power-level-dBmV*] **Example:** `Router(config)# cable spectrum-group 4 time Monday 12:00:00 frequency 40000000`	Creates the spectrum group (if it does not already exist), and adds the specified fixed frequency to the group.
Step 4	**cable spectrum-group** *group-number* [**time** *day hh:mm:ss*] **band** *up-freq-Hz up-freq2-Hz [power-level-dBmV*]	Creates the spectrum group (if it does not already exist), and adds the specified band of frequencies to the group.

	Command or Action	Purpose
	Example: `Router(config)# cable spectrum-group 4 band 20000000 24000000 13`	**Note** Repeat Step 3, on page 593 and Step 4, on page 593 as needed for each fixed frequency and frequency band that should be a member of this spectrum group. You must assign at least two fixed frequencies, or a frequency band that contains at least two center frequencies, to a spectrum group before frequency hopping can occur.
Step 5	**cable spectrum-group** *group-number* **hop period** *seconds* **Example:** `Router(config)# cable spectrum-group 4 hop period 60`	Specifies the minimum time, in seconds, between frequency hops. **Note** We recommend a configuration of 30 seconds when using a Cisco uBR-MC5X20S/U/H BPE.
Step 6	**cable spectrum-group** *group-number* **hop threshold** [*percent*] **Example:** `Router(config)# cable spectrum-group 4 hop threshold 25`	Specifies the frequency hop threshold for a spectrum group. • **percent—**(Optional) Frequency hop threshold as a percentage of station maintenance messages that are lost. Valid range is from 1 to 100 percent, with a default of 50 percent.
Step 7	**cable spectrum-group** *group-number* **shared** **Example:** `Router(config)# cable spectrum-group 4 shared`	(Optional) Specifies that the upstream ports in a spectrum group should use a unique upstream frequency.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Assigning a Spectrum Group to One or More Upstream Ports

After a spectrum group has been created and configured, you must assign it to one or more upstream ports before the group's frequency spectrum is used for frequency hopping. You can assign a spectrum group to an upstream in the following ways:

- Use the **cable spectrum-group** interface configuration command to assign a spectrum group to all of the upstreams on a cable interface.
- Use the **cable upstream spectrum-group** interface configuration command to assign a spectrum group to one individual upstream. This command overrides a group that might have been assigned to all of the upstreams on the interface by the **cable spectrum-group** command.

To assign a spectrum group to one or all upstream ports on an interface, use the following procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Use one of the following commands: • **interface cable** *x/y* • **interface cable** *x/y/z* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 4	**cable spectrum-group** *group-number* **Example:** `Router(config-if)# cable spectrum-group 4`	Assigns the specified spectrum group as the default group for all upstreams on this cable interface. The valid range for *group-number* is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.
Step 5	**cable upstream** *n* **spectrum-group** *group-number* **Example:** `Router(config-if)# cable upstream 1 spectrum-group 5`	Assigns the specified spectrum group to this individual upstream, overriding any previous assignment that was done for all upstreams on the interface using the **cable spectrum-group** command. **Note** Repeat this step for each upstream to be configured. **Note** Repeat Step 3, on page 595 through Step 5, on page 595 for each cable interface to be configured.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Note For help in determining which upstream ports to assign in a combiner group, refer to the, Example: Determining the Upstream Ports Assigned to a Combiner Group, on page 623.

Tip To verify the spectrum group configuration, use the **show cable spectrum-group** command in privileged EXEC mode.

Configuring Shared Spectrum Groups (Fiber Node Groups) for DOCSIS 3.0

Cisco IOS Release 12.3(21)BC, and later releases, support shared spectrum groups, otherwise known as fiber node groups, for DOCSIS 3.0 on the Cisco uBR10012 router.

This feature supports shared spectrum groups that cross multiple cable interface line cards on the Cisco CMTS router, and shared spectrum groups within a single cable interface line card.

For additional information about configuring fiber node groups on the Cisco CMTS, see:

- Creating and Configuring Spectrum Groups, on page 592
- Assigning a Spectrum Group to One or More Upstream Ports, on page 594
- Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide

Configuring Dynamic Upstream Modulation (MER [SNR]-Based)

To use the Dynamic Upstream Modulation feature on cable interface line cards that support only the MER (SNR) version of this feature, you must do the following:

1. Create a primary modulation profile. This typically is a more bandwidth-efficient but a less robust profile.
2. Optionally create a secondary modulation profile. This typically is a less bandwidth-efficient but a moderately robust profile.
3. Optionally create a tertiary modulation profile. This typically is a less bandwidth-efficient but a more robust profile.
4. Assign the profiles to the desired cable interfaces and upstreams.

Tip When creating the modulation profiles, we recommend that you use the predefined modulation profiles, as opposed to manually specifying each burst parameter for each modulation profile.

Restriction

- The Dynamic Upstream Modulation feature is supported only for DOCSIS 1.0 or DOCSIS 1.1 TDMA-only modulation profiles for advanced spectrum management.
- The DOCSIS 2.0 mixed-mode or ATDMA-only mode modulation profiles are supported only for basic spectrum management (MER [SNR]-based) and not for advanced spectrum management.
- The Three Step Dynamic Modulation feature supports only basic spectrum management features. It does not support modulation profile changes based on CNR (CNiR) thresholds and CNR (CNiR) measurements.
- The Dynamic Upstream Modulation feature is not enabled for single modulation profile configurations.
- You can configure only two modulation profiles when an upstream is already assigned to a spectrum group for frequency hopping. The spectrum group here implies advanced spectrum management and/or the use of CNR (CNiR).
- A single profile is automatically removed from the configuration if three modulation profiles are assigned to an upstream interface before assigning spectrum group, based on the following conditions:
  - The robust profile is dropped if the upstream port is using a high performance profile.
  - The high performance profile is dropped if the upstream port is using a mid-level or robust profile.

To create and assign the primary, secondary, and tertiary modulation profiles to an upstream, use the following procedures.

Starting with Cisco IOS Release 12.2(33)SCC, you can configure two logical channels on a single physical port for the uBR10012 router. When you configure logical channels, the upstream related commands are categorized into two groups: physical port level and logical channel level.

Physical Port Level

Physical port level commands use the format of **cable upstream** *n, where* n denotes the physical port number.

Logical Channel Level

Logical channel level commands use the format of **cable upstream** *n m, where* n denotes the physical port number, and m denotes the logical channel index number of 0 or 1.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable modulation-profile** *profile* {**mix** | **qam-64** | **qam-16** | **qpsk** | **robust-mix**} **Example:** `Router(config)# cable modulation-profile 3 mix`	Creates the primary modulation profile for use on a DOCSIS 1.0 or DOCSIS 1.1 TDMA or A-TDMA upstream. Typically, the primary profile is either **qam-16** or **mix**. **Note** Repeat this command to create the secondary and tertiary profile for use on a DOCSIS 1.0 or DOCSIS 1.1 TDMA or A-TDMA upstream. Typically, the secondary and tertiary profiles are either **robust-mix** or **qpsk**. **Note** You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.
Step 4	Use one of the following commands: • **interface cable** *x/y* • **interface cable** *x/y/z* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 5	**cable upstream** *n* **modulation-profile** *primary-profile-number* [*secondary-profile-number*] [*tertiary-profile-number*] **Example:** `Router(config-if)# cable upstream 0 modulation-profile 3 4 5`	Assigns a primary modulation profile, and the optional secondary and tertiary modulation profiles, to the specified upstream port. **Note** For Cisco IOS Release 12.3(13a)BC and later, the MER (SNR), correctable FEC, uncorrectable FEC thresholds, and hysteresis can be user defined using the steps from Step 6, on page 598 to Step 9, on page 599.
Step 6	Use one of the following commands: • **cable upstream** *n* **threshold snr-profiles** *threshold1-in-db threshold2-in-db* • **cable upstream** *n m* **threshold snr-profiles** *threshold1-in-db threshold2-in-db* **Example:** `Router(config-if)# cable upstream 0 threshold snr-profiles 25 15`	(Optional) Specifies the MER (SNR) threshold in dB.
Step 7	Use one of the following commands: • **cable upstream** *n* **threshold corr-fec** *corr-fec* • **cable upstream** *n m* **threshold corr-fec** *corr-fec*	(Optional) Specifies the allowable number of correctable FEC errors for the upstream.

	Command or Action	Purpose
	Example: `Router(config-if)# cable upstream n threshold corr-fec 20`	
Step 8	Use one of the following commands: • **cable upstream** *n* **threshold uncorr-fec** *uncorr-fec* • **cable upstream** *n m* **threshold uncorr-fec** *uncorr-fec* **Example:** `Router(config-if)# cable upstream n threshold uncorr-fec 10`	(Optional) Specifies the allowable number of uncorrectable FEC errors for the upstream.
Step 9	**cable upstream** *n* **threshold hysteresis** *hysteresis-in-db* **Example:** `Router(config-if)# cable upstream n threshold hysteresis 10`	(Optional) Specifies the hysteresis value to be used in conjunction with the dynamic modulation upgrade thresholds.
Step 10	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Tip See the Dynamic Upstream Modulation (MER [SNR]-Based), on page 584 for a complete description of the Dynamic Upstream Modulation feature.

Verifying Frequency Hopping

You can verify frequency hopping on the CMTS by using the command-line interface (CLI).

For Cisco IOS Release 12.3(13a)BC and later releases, two more show commands have been added:

- **show cable hop upstream history**
- **show cable hop upstream threshold**

Verifying Frequency Hopping Using CLI Commands

To verify frequency hopping using CLI commands, use the following procedure:

Step 1 Verify that the interface being tested is up, using the **show interfaces cable** command in privileged EXEC mode. The first line of the output shows whether both the interface and line protocol are up.

Example:

```
Router# show interfaces cable 6/0

Cable6/0 is up, line protocol is up
  Hardware is BCM3210 ASIC, address is 000a.13e8.1ca8 (bia 000a.13e8.1ca8)
  Internet address is 10.20.114.33/27
  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec,
```

Step 2 Verify that the upstream being tested is up, using the **show interfaces cable upstream** command. The first line shows whether the upstream is up.

Example:

```
Router# show interfaces cable 6/0 upstream 5

Cable6/0: Upstream 5 is up
     Received 8 broadcasts, 0 multicasts, 6388105 unicasts
     0 discards, 0 errors, 0 unknown protocol
     6388113 packets input, 0 uncorrectable
     0 noise, 0 microreflections
     Total Modems On This Upstream Channel : 23 (22 active)
```

Step 3 Use the **show cable hop upstream** command to display the frequency that the upstream is currently using:

Example:

```
Router# show cable hop cable 6/0 upstream 5

Upstream    Port       Poll Missed Min    Missed Hop   Hop     Corr    Uncorr
Port        Status     Rate Poll   Poll   Poll   Thres Period  FEC     FEC
                       (ms) Count  Sample Pcnt   Pcnt  (sec)   Errors  Errors
Cable6/0/U5 16.816 Mhz 1000 0      10         0%   20%  25     0       0
```

Step 4 Use the **show cable hop upstream history** command to display the frequency change, modulation change, and channel width change action history of the upstreams:

Example:

```
Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 26.358 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

Note Cisco IOS Release 12.3(23)BC7 modifies the **show cable hop upstream history** command to show the identifier for the modulation profile.

Step 5 Use the **show cable hop upstream threshold** command to display the user-defined thresholds and current CNR, MER (SNR), correctable FEC percentage, uncorrectable FEC percentage, and missed station maintenance percentage values of the upstreams:

Example:

```
Router# show cable hop cable 6/0/0 upstream threshold

Upstream   SNR(dB)          CNR(dB)          CorrFEC%  UncorrFEC%        MissedSM%
Port       Val Thre1 Thre2 Val Thre1 Thre2 Pcnt Thre Pcnt Thre         Pcnt Thre

Ca6/0/0/U0 27   25   15    39   35   25    0    3    0    1           75   75
Ca6/0/0/U1 31   25   15    51   35   25    0    3    0    1           90   75
Ca6/0/0/U2 --   35   25    --   35   25    0    3    0    1           0    75
Ca6/0/0/U3 --   35   25    --   35   25    0    3    0    1           0    75
```

Step 6 Use the **test cable hop** command to force the desired upstream to perform a frequency hop. A few seconds after giving the command, a console message should appear informing you of the hop. Repeat the command as needed to verify that the upstream hops through all the frequencies that have been assigned to the upstream's spectrum group.

Example:

```
Router# test cable hop cable 6/0 upstream 5

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 15.760 MHz

Router# test cable hop cable 6/0 upstream 5

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 26.832 MHz
```

Step 7 Use the **test cable channel-width** command to force the desired upstream to perform a channel-width change. A few seconds after giving the test command, use the show cable hop command to verify the channel-width change.

Example:

```
Router# test cable channel-width cable 7/0/0 upstream 0

Channel width changed to 1600000 Hz for Cable7/0/0 U0

Router# *Sep 17 17:06:46.882: %UBR10000-5-USCWCHG: Interface Cable7/0/0 U0, channel width changed
to 1600 kHz SLOT 7/0: Sep 17 17:06:46.898: %UBR10000-5-USCWCHG: Interface Cable7/0/0 U0, channel
width changed to 1600 kHz

Router# Sep 17 17:06:46.898: %Interface Cable7/0/0 U0 With channel width 1600 kHz, the minislot size
 is now changed to 4 ticks.

Router# show cable hop cable 7/0/0 upstream 0 history


F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:06:46 C  3.2    1.6    Test command enforced
             Sep 17 17:06:02 M  222    221    SNR 36>=28 CFEC 0<=3 UnCFEC 0<=1
             Sep 17 17:06:00 M  221    222    Test command enforced
             Sep 17 17:03:21 M  222    221    SNR 36>=28 CFEC 0<=3 UnCFEC 0<=1
             Sep 17 17:03:19 M  221    222    Test command enforced
             Sep 17 17:01:44 F  26.358 19.742 Test command enforced
             Sep 17 17:01:17 F  21.528 26.358 Test command enforced
             Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 21.528 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

```
Router#
```

Step 8 Use the **test cable freq-hop** command to force the desired upstream to perform a dynamic frequency change. A few seconds after giving the test command, use the **show cable hop** command to verify the frequency change.

Example:

```
Router# test cable freq-hop cable 7/0/0 upstream 0

SLOT 7/0: Sep 17 17:01:44.650: %UBR10000-5-USFREQCHG: Interface Cable7/0/0 U0, changed to Freq 19.742
 MHz

Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:01:44 F  26.358 19.742 Test command enforced
             Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 26.358 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

Step 9 Use the **test cable modulation-change** command to force the desired upstream to perform a dynamic modulation change. A few seconds after giving the test command, use the **show cable hop** command to verify the modulation change.

Example:

```
Router# test cable modulation-change cable 7/0/0 upstream 0

SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-5-USMODCHANGE: Interface Cable7/0/0 U0, dynamic modulation
 changed to QPSK
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: request burst's preamble length in mod
profile 222 is adjusted to 38 bits.
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: initial burst's preamble length in mod
profile 222 is adjusted to 100 bits.
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: station burst's preamble length in mod
profile 222 is adjusted to 100 bits.

Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:03:19 M  221    222    Test command enforced
             Sep 17 17:01:44 F  26.358 19.742 Test command enforced
             Sep 17 17:01:17 F  21.528 26.358 Test command enforced
             Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 21.528 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

Troubleshooting Spectrum Group Characteristics

To troubleshoot the configuration, make sure that you entered a valid spectrum group number, time, frequency, and input power level. Also, when defining your spectrum, use the following guidelines:

- Avoid frequencies with known ingress problems, such as amateur radio bands or short-wave bands.
- Avoid a hostile spectrum below 20 MHz.
- Allow extra bands for frequency hopping.

- Place upstream ports in the same combiner group in a shared spectrum group.
- Use the receive power level setting to perform slight equalization adjustments.

Intelligent and Advanced Spectrum Management Configuration Tasks

The following sections describe the configuration tasks that are needed to configure a Cisco uBR7200 series or Cisco uBR10012 universal broadband router for the intelligent and advanced spectrum management features that are available with the Cisco cable interface line cards.

Configuring and Assigning Spectrum Groups

You must create and configure a spectrum group before you can use the intelligent and advanced spectrum management features. These procedures are the same as those used for guided and scheduled spectrum management, which are given in the following sections:

- Creating and Configuring Spectrum Groups, on page 592
- Assigning a Spectrum Group to One or More Upstream Ports, on page 594

After the spectrum groups have been configured and assigned to upstreams, the Cisco IOS software automatically uses the advanced frequency hopping algorithms on the cable interface line cards that support it.

Note For efficient use of the intelligent and advanced spectrum management features, we recommend configuring only frequency bands, and not fixed frequencies, when creating spectrum groups. A spectrum group must contain a frequency band that is wide enough for the cable interface to find at least two center frequencies at the configured channel width, before frequency hopping can occur.

Configuring Dynamic Upstream Modulation (CNR-Based)

Configuring the CNR-based version of the Dynamic Upstream Modulation feature is similar to configuring the MER (SNR)-version of this feature:

1. Create a primary modulation profile. This typically is a more bandwidth-efficient but a less robust profile.
2. Create a secondary modulation profile. This typically is a less bandwidth-efficient but a more robust profile.

Tip When creating the modulation profiles, we recommend that you use the predefined modulation profiles, as opposed to manually specifying each burst parameter for each modulation profile.

3. Assign the profiles to the desired cable interfaces and upstreams.

After the modulation profiles have been created and assigned to upstreams, the Cisco IOS software automatically uses the advanced CNR-based version of the Dynamic Upstream Modulation feature on the cable interface line cards that support it.

Restriction

- The Dynamic Upstream Modulation feature is supported only for DOCSIS 1.0 or DOCSIS 1.1 TDMA-only modulation profiles. It is not supported for DOCSIS 2.0 mixed-mode or A-TDMA-only mode modulation profiles.
- If you are using a software release between Cisco IOS Release 12.2(8)BC2 and Cisco IOS Release 12.2(11)BC2 inclusive, you must perform an additional configuration when using the **mix** and **qam-16** predefined modulation profiles. This is because the short and long grant bursts of the **mix** and **qam-16** profiles default to a unique word offset of 8 (uw8). These values should be changed to **uw16** for optimal performance. To do this, first create the modulation profiles using the procedure given in this section, and then issue the following commands for each modulation profile that uses the **mix** or **qam-16** predefined modulation profiles:

```
cable modulation-profile n short 6 75 6 8 16qam scrambler 152 no-diff 144
fixed uw16
cable modulation-profile n long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

Note The defaults for these predefined profiles were corrected in Cisco IOS Release 12.2(11)BC3 and later releases, and this step is no longer needed.

- Three Step Dynamic Modulation is not supported on the CNR-based version of dynamic upstream modulation.
- The CNR-based Dynamic Upstream Modulation feature does not support A-TDMA modulation profiles. However, A-TDMA is supported in the MER (SNR)-based Dynamic Upstream Modulation feature.

To assign the primary and secondary profiles to an upstream, use the following procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk** | **robust-mix**} **Example:** `Router(config)# cable modulation-profile 3 mix`	Creates the primary modulation profile for use on a DOCSIS 1.0 or DOCSIS 1.1 TDMA upstream. Typically, the primary profile is either **qam-16** or **mix**. **Note** Repeat this command to create the secondary profile for use on a DOCSIS 1.0 or DOCSIS 1.1 TDMA upstream. Typically, the secondary profile is either **robust-mix** or **qpsk**.

	Command or Action	Purpose
		Note You can also create custom modulation profiles with the **cable modulation-profile** command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.
Step 4	Use one of the following commands: • **interface cable** *x/y* • **interface cable** *x/y/z* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 5	**cable upstream** *n* **modulation-profile** *primary-profile-number secondary-profile-number* **Example:** `Router(config-if)# cable upstream 0 modulation-profile 3 4`	Assigns a primary modulation profile, and an optional secondary modulation profile, to the specified upstream port.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Proactive Channel Management

The cable interface line cards that support the advanced spectrum management features can be configured with the following parameters to fine-tune the operation of proactive channel management on the upstreams of the cards:

- Priority of the corrective actions to be taken when noise on an upstream exceeds the threshold for its modulation profile.
- CNR (CNiR) and MER (SNR) threshold and FEC values for the upstream and its two modulation profiles.
- Allowable range of channel widths that can be used if frequency hopping or modulation switching cannot avoid the upstream problems.

These parameters all have default settings, so you do not need to perform this procedure unless you want to change these parameters to better match the characteristics of your physical plant.

A major exception to this is if you are using only one modulation profile and are using a software release prior to Cisco IOS Release 12.2(8)BC2. In these releases, a frequency hop would occur if just one of the measured values (CNR [CNiR] value, correctable FEC counter, or uncorrectable FEC counter) crosses the

configured threshold value. Because of this, if you are using only one modulation profile (QPSK) with one of these software releases, you might need to reduce the CNR (CNiR) threshold value and increase the correctable FEC error value to prevent undesired frequency hopping.

Note This situation no longer occurs in Cisco IOS Release 12.2(8)BC2 and later releases, because a frequency hop can occur only when both the CNR (CNiR) value and one of the FEC counters falls below the threshold value.

To configure the parameters, use the following procedure.

Note Starting with Cisco IOS Release 12.3(13a)BC, the **cable upstream** *n* **threshold** command was changed to provide more functionality.

Configuring Proactive Channel Management for Releases Prior to 12.3(13a)BC

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Use one of the following commands: • **interface cable** *x/y* • **interface cable** *x/y/z* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 4	Use one of the following commands: • **cable upstream** *n* **hop-priority frequency modulation channel-width** • • **cable upstream** *n* **hop-priority modulation frequency channel-width** • • **cable upstream** *n* **hop-priority frequency channel-width modulation**	Specifies the priority of the three types of corrective actions (**modulation**, **frequency**, and **channel-width**) to be taken when the noise for the upstream exceeds the threshold specified for the current modulation profile. The default priority is **frequency**, **modulation**, and **channel-width**. • *n* —Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. **Note** The **channel-width** option must always appear after the **frequency** option.

	Command or Action	Purpose
	Example: `Router(config-if)# cable upstream 0 hop-priority frequency channel-width modulation`	
Step 5	**cable upstream** *n* **threshold cnr-profile1** *threshold1-in-db* **cnr-profile2** *threshold2-in-db* **corr-fec** *fec-corrected* **uncorr-fec** *fec-uncorrected* **Example:** `Router(config-if)# cable upstream 5 threshold cnr-profile1 20 cnr-profile2 10 corr-fec 5 uncorr-fec 1`	Specifies the CNR (CNiR) threshold and FEC values for the upstream and its two modulation profiles. • *n* —Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. • **cnr-profile1** *threshold1-in-db* —Specifies the CNR (CNiR) threshold for the primary modulation profile (5 to 35 dB, with a default of 25). • **cnr-profile2** *threshold2-in-db* —Specifies the CNR (CNiR) threshold for the secondary modulation profile (5 to 35 dB, must be less than that for the primary modulation profile, with a default of 13). • **corr-fec** *fec-corrected* —Specifies the permitted number of correctable FEC errors for the upstream, which is the percentage of total packets received on the upstream during the polling period. The valid range is from 0 to 30 percent of total packets, and a default of 3 percent. • **uncorr-fec** *fec-uncorrected* —Specifies the permitted number of uncorrectable FEC errors for the upstream, which is the percentage of total packets received on the upstream during the polling period. The valid range is from 0 to 30 percent of total packets, with a default of 1 percent. **Note** For normal plant use, we recommend that the uncorrectable FEC threshold remain at its default of 1 percent to avoid an unacceptable number of errors on the channel.
Step 6	**cable upstream** *n* **channel-width** *first-choice-width* [*last-choice-width*] **Example:** `Router(config-if)# cable upstream 0 channel-width 800000 800000`	Specifies the range of allowable channel widths that can be used when ingress noise conditions require changing the channel width. The upstream begins with the first-choice channel width and decreases in half until it hits the secondary channel width. • *first-choice-width* —Upstream channel width in hertz (Hz). The valid values are: • 200,000 (160,000 symbols/sec) • 400,000 (320,000 symbols/sec) • 800,000 (640,000 symbols/sec) • 1,600,000 (1,280,000 symbols/sec) (Default) • 3,200,000 (2,560,000 symbols/sec) • 6,400,000 (5,120,000 symbols/sec) (DOCSIS 2.0 A-TDMA-only upstreams only)

	Command or Action	Purpose
		• *last-choice-width* —(Optional) Upstream channel width in hertz. Supports the same values as *first-choice-width*, but must be less than or equal to *first-choice-width* . **Note** Repeat Step 4, on page 606 through Step 6, on page 607 for each upstream to be configured.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Proactive Channel Management for Release 12.3(13a)BC, 12.2(33)SCC, and Later

Starting with Cisco IOS Release 12.2(33)SCC, you can configure two logical channels on a single physical port of the uBR10012 universal broadband router. When you configure logical channels, the upstream related commands are categorized into two groups: physical port level and logical channel level.

Physical Port Level

Physical port level commands use the format of **cable upstream** *n*, where *n* denotes the physical port number.

Logical Channel Level

Logical channel level commands use the format of **cable upstream** *n m* , where *n* denotes the physical port number, and *m* denotes the logical channel index number of 0 or 1.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Use one of the following commands: • **interface cable** *x/y* • **interface cable** *x/y/z* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	Use one of the following commands: • **cable upstream** *n* **hop-priority frequency modulation channel-width** • • **cable upstream** *n* **hop-priority modulation frequency channel-width** • • **cable upstream** *n* **hop-priority frequency channel-width modulation** **Example:** `Router(config-if)# cable upstream 0 hop-priority frequency channel-width modulation`	Specifies the priority of the three types of corrective actions (**modulation**, **frequency**, and **channel-width**) to be taken when the noise for the upstream exceeds the threshold specified for the current modulation profile. The default priority is **frequency**, **modulation**, and **channel-width**. • *n*—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. **Note** The **channel-width** option must always appear after the **frequency** option.
Step 5	**cable upstream** *n* **threshold cnr-profiles** *threshold1-in-db threshold2-in-db* **Example:** `Router(config-if)# cable upstream 2 threshold  cnr-profiles 23 14`	(Optional) Specifies the CNR (CNiR) threshold and FEC values for the upstream and its two modulation profiles. • *threshold1-in-db*—CNR (CNiR) threshold for the primary modulation profile (5 to 35 dB, with a default of 25). • *threshold2-in-db*—CNR (CNiR) threshold for the secondary modulation profile (5 to 35 dB, must be less than that for the primary modulation profile, with a default of 15). **Note** To bypass both the primary and secondary CNR (CNiR) thresholds, set the first parameter (*threshold1-in-db*) to 0. This disallows the second parameter (*threshold2-in-db*), enabling you to bypass both the CNR (CNiR) thresholds.
Step 6	Use one of the following commands: • **cable upstream n upstream threshold snr-profiles** *threshold1-in-db threshold2-in-db* • • **cable upstream** *n m* **upstream threshold snr-profiles** *threshold1-in-db threshold2-in-db* • **Example:** `Router(config-if)# cable upstream 2 threshold  snr-profiles 23 14`	(Optional) Specifies the MER (SNR) threshold and FEC values for the upstream and its two modulation profiles. • *m*—Logical channel index. Valid values are 0 and 1. • *threshold1-in-db*—MER (SNR) threshold for the primary modulation profile (5 to 35 dB, with a default of 25) • *threshold2-in-db*—MER (SNR) threshold for the secondary modulation profile (5 to 35 dB, must be less than that for the primary modulation profile, with a default of 15) **Note** You can bypass the primary MER (SNR) threshold (*threshold1-in-db*) by setting it to 0. However, you must enter the second parameter (*threshold2-in-db*).
Step 7	**cable upstream** *n* **threshold hysteresis** *hysteresis-in-db*	(Optional) Specifies the hysteresis value to be used in conjunction with the dynamic modulation upgrade thresholds.

	Command or Action	Purpose
	Example: `Router(config-if)# cable upstream 2 threshold hysteresis 3`	• **hysteresis** *hysteresis-in-db*—Permitted number of hysteresis value to be used in conjunction with the dynamic modulation upgrade thresholds. The valid range is 0 to 10. **Note** You can bypass the **hysteresis** threshold by setting the value to 0.
Step 8	Use one of the following commands: • **cable upstream** *n* **threshold corr-fec** *corrfec-threshold* • **cable upstream** *n m* **threshold corr-fec** *corrfec-threshold* **Example:** `Router(config-if)# cable upstream 5 threshold  corr-fec 5`	(Optional) Specifies the CNR (CNiR) threshold and FEC values for the upstream and its two modulation profiles. • *corrfec-threshold*—Permitted number of correctable FEC errors for the upstream, which is the percentage of the total packets received on the upstream during the polling period. The valid range is from 0 to 30 percent of total packets, and a default of 3 percent. **Note** You can bypass the **corr-fec** threshold by setting the value to 0.
Step 9	Use one of the following commands: • **cable upstream** *n* **threshold uncorr-fec** *uncorrfec-threshold* • **cable upstream** *n m* **threshold uncorr-fec** *uncorrfec-threshold* **Example:** `Router(config-if)# cable upstream 5 threshold  uncorr-fec 1`	(Optional) Specifies the CNR (CNiR) threshold and FEC values for the upstream and its two modulation profiles. • *uncorrfec-threshold*—Permitted number of uncorrectable FEC errors for the upstream, as given as a percentage of total packets received on the upstream during the polling period. The valid range is 0 to 30 percent of total packets, with a default of 1 percent. **Note** You can bypass the un**corr-fec** threshold by setting the value to 0. **Note** For normal plant use, we recommend that the uncorrectable FEC threshold remain at its default of 1 percent to avoid an unacceptable number of errors on the channel.
Step 10	**cable upstream** *n* **channel-width** *first-choice-width* [*last-choice-width*] **Example:** `Router(config-if)# cable upstream 0 channel-width 800000 800000`	(Optional) Specifies the range of allowable channel widths that can be used when ingress noise conditions require changing the channel width. The upstream begins with the first-choice channel width and decreases in half until it hits the secondary channel width. • *first-choice-width*—Upstream channel width in hertz (Hz). The valid values are: • 200,000 (160,000 symbols/sec) • 400,000 (320,000 symbols/sec) • 800,000 (640,000 symbols/sec) • 1,600,000 (1,280,000 symbols/sec) (Default) • 3,200,000 (2,560,000 symbols/sec) • 6,400,000 (5,120,000 symbols/sec) (DOCSIS 2.0 A-TDMA-only upstreams only)

	Command or Action	Purpose
		• *last-choice-width*—(Optional) Upstream channel width in hertz. Supports the same values as *first-choice-width* , but must be less than or equal to *first-choice-width* . **Note** Repeat Step 4, on page 609 through Step 10, on page 610 for each upstream to be configured.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Spectrum Management Configuration

Follow the steps given below to verify the spectrum management configuration.

Step 1 To check the value of the settings you have entered, use the **show running-config** command in privileged EXEC mode:

Example:
```
Router# show running-config
```

Step 2 To display the configuration for each modulation profile, use the **show cable modulation-profile** command in privileged EXEC mode:

Example:
```
Router# show cable modulation-profile
```

To display the configuration for a specific modulation profile, add the profile number to the **show cable modulation-profile** command in privileged EXEC mode:

Example:
```
Router# show cable modulation-profile 6
```

Step 3 To display the status and configuration of each upstream, use the **show controllers cable upstream** command in privileged EXEC mode. The following example displays information for upstreams 0 on a cable line card:

Example:
```
Router# show controller cable 8/1/14 upstream 0

 Cable8/1/14 Upstream 0 is up
  Frequency 19.504 MHz, Channel Width 3.200 MHz, Symbol Rate 2.560 Msps
  Modulations (64-QAM) - A-short 64-QAM, A-long 64-QAM, A-ugs 64-QAM
  Mapped to shared connector 18 and receiver 56
  Spectrum Group 8
  MC3Gx60  CNR measurement : 30 dB
  US phy MER(SNR)_estimate for good packets - 32.5530 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 1547
  Ranging Backoff Start 3, Ranging Backoff End 6
```

```
US timing offset adjustment type 0, value 0
Ranging Insertion Interval automatic (60 ms)
US throttling off
Tx Backoff Start 3, Tx Backoff End 5
Modulation Profile Group 221
Concatenation is enabled
Fragmentation is enabled
part_id=0x3142, rev_id=0xC0, rev2_id=0x00
nb_agc_thr=0x0000, nb_agc_nom=0x0000
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 2
Minislot Size in Symbols = 32
Bandwidth Requests = 0xEE3AF
Piggyback Requests = 0x6A24F
Invalid BW Requests= 0x76
Minislots Requested= 0xC33362
Minislots Granted  = 0x158609
Minislot Size in Bytes = 24
Map Advance (Dynamic) : 2581 usecs
Map Count Internal = 330309891
No MAP buffer= 0x0   No Remote MAP buffer= 0x0
Map Counts: Controller 8/1/0 = 1321230158
UCD Counts:
  Controller 8/1/0:0 = 336057
  Controller 8/1/0:1 = 336057
  Controller 8/1/0:2 = 336057
  Controller 8/1/0:3 = 336057

UCD procedures on lch 0
UCD ucd-succeeds(5) ucd-shut(0) init-state-err(0)
UCD init-tss-err(0) init-timeout(0) init-start-err(0)
UCD ucd-ccc-time(0) ucd-timeout(0) ucd-tss-err(0)
UCD ucd-state-err(0) ucd-process(0) ucd-retries(0)
UCD stale-tss(0)
ATDMA mode enabled
PHY: us errors 0  us recoveries 0 (enp 0)
MAC PHY TSS: tss error start 0  tss error end 0
MAC PHY Status: bcm3140 status 0  lookout status 0
PHY: TSS late 0  discontinuous 0
PHY: TSS mis-match 0  not-aligned 0
PHY: TSS missed snapshots from phy 0
MAP/UCD Replication Instructions:
  Controller 8/1/0 index = 477, bitmap = 0x000F
Dynamic Services Stats:
DSA: 0  REQs  0 RSPs  0 ACKs
0 Successful DSAs  0 DSA Failures
DSC: 0  REQs  0 RSPs  0 ACKs
0 Successful DSCs  0 DSC Failures
DSD:  0 REQs  0 RSPs
0 Successful DSDs  0 DSD Failures
Dropped MAC messages: (none)
```

Step 4 To display the hop period and hop threshold values for each upstream, use the **show cable hop** command in privileged EXEC mode:

Example:

```
Router# show cable hop

 Upstream    Port       Poll Missed Min    Missed Hop   Hop     Corr    Uncorr
 Port        Status     Rate Poll   Poll   Poll   Thres Period  FEC     FEC
                        (ms) Count  Sample Pcnt   Pcnt  (sec)   Errors  Errors
Cable3/0/U0 20.800 Mhz 105  0      20         0%   25%  45     1       4
Cable3/0/U1 20.800 Mhz 105  0      48         0%   25%  45     2       19
Cable3/0/U2 23.120 Mhz 105  0      45         0%   25%  45     0       5
Cable3/0/U3 22.832 Mhz 105  0      26         0%   25%  45     0       6
Cable3/0/U4 22.896 Mhz 105  0      43         0%   25%  45     0       7
Cable3/0/U5 23.040 Mhz 105  0      54         0%   25%  45     1       3
Cable4/0/U0 22.896 Mhz 117  0      26         0%   25%  45     0       2
```

```
Cable4/0/U1 23.168 Mhz 117  0      87         0%   25%  45     4       2
Cable4/0/U2 22.896 Mhz 117  0      23         0%   25%  45     1       0
Cable4/0/U3 20.800 Mhz 117  0      54         0%   25%  45     0       0
Cable4/0/U4 22.928 Mhz 117  0      22         0%   25%  45     0       1
Cable4/0/U5 22.960 Mhz 117  0      0       -----   25%  45     0       0
```

Step 5 To display changes from one state to another, at any time and for any reason, for frequency, modulation, and channel width, use the **history** option of the **show cable hop** command.

Example:

```
Router# show cable hop c8/1/1 u0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream   Action             Chg    Chg    Action
Port       Time          Code From   To     Reason
C8/1/1 U0  Feb 20 12:21:29 M  142    141    SNR 28>=28 CFEC 0<=3 UnCFEC 0<=1
           Feb 20 12:09:08 F   0.000 24.000 Configuration changed
```

Step 6 To display thresholds for MER (SNR), CNR (CNiR), and FEC, use the **threshold** option of the **show cable hop** command.

Example:

```
Router# show cable hop c8/1/1 u0 threshold

Upstream   SNR(dB)          CNR(dB)          CorrFEC%  UncorrFEC%       MissedSM%
Port       Val Thre1 Thre2 Val Thre1 Thre2 Pcnt Thre Pcnt Thre        Pcnt Thre
C8/1/1 u0  33   23   14    60   25   15    0    1    0    2           0    50
```

Step 7 To display the assignment of each spectrum group, use the **show cable spectrum-group** command in privileged EXEC mode:

Example:

```
Router# show cable spectrum-group

Group  Frequency      Upstream     Weekly Scheduled            Power   Shared
No.    Band           Port         Availability                Level   Spectrum
       (Mhz)                       From Time:    To Time:      (dBmV)
1      20.000-21.600                                          0       No
1      22.000-24.000                                          0       No
1      20.784 [1.60]  Cable3/0 U0                             0
1      20.784 [1.60]  Cable3/0 U1                             0
1      23.120 [1.60]  Cable3/0 U2                             0
1      22.832 [1.60]  Cable3/0 U3                             0
1      22.896 [1.60]  Cable3/0 U4                             0
1      23.024 [1.60]  Cable3/0 U5                             0
1      23.152 [1.60]  Cable4/0 U1                             0
1      22.896 [1.60]  Cable4/0 U0                             0
1      22.896 [1.60]  Cable4/0 U2                             0
1      20.784 [1.60]  Cable4/0 U3                             0
1      22.928 [1.60]  Cable4/0 U4                             0
1      22.960 [1.60]  Cable4/0 U5                             0
```

Step 8 To display the current CNR (CNiR) value for a particular cable modem, use the **show cable modem cnr** command in privileged EXEC mode:

Example:

```
Router# show cable modem 5.100.1.94 cnr

MAC Address    IP Address      I/F          MAC          Prim  snr/cnr
                                            State        Sid   (dB)
0018.689c.17b8 5.100.1.94      C7/0/0/U1    online       428   36.12
```

Note Starting Cisco IOS Release 12.2(33)SCF, the output of the **show cable modem cnr** command will always display CNR (CNiR) values for all the US channels for a specific CM, irrespective of whether spectrum management is enabled or not for the US channels. For all the releases prior to Cisco IOS Release 12.2(33)SCF, the command output will display CNR (CNiR) when you use specific groups, otherwise it will be MER (SNR).

Monitoring Spectrum Management

You can use Cisco IOS CLI commands to monitor spectrum management activity on the Cisco CMTS. If you are using Cisco IOS Release 12.2(8)BC2 or later 12.2 BC releases, you can also use SNMP to monitor the spectrum management activity.

Note When using the Cisco uBR10-MC5X20S/U/H BPE you must also use Cisco IOS Release 12.3(13a)BC or a later release.

See the following sections for more information:

Using CLI Commands

The following commands provide information on the spectrum condition of an upstream:

Command	Purpose
Router# **show cable hop**[**cable***x/y*] [**upstream** *usport*]	Displays the hop period and hop threshold values, as well as the FEC error counters, for all upstreams in the router, all upstreams on one cable interface line card, or a single upstream.
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*][*thresholds*]	Displays the configured and current value of MER (SNR) in dB, CNR (CNiR) in dB, CorrFEC in percentage, UncorrFEC in percentage, and missed station maintenance in percentage for a specified upstream. **Note** Supported in Cisco IOS Release 12.3(13a)BC or later release.
Router# **show cable hop history**	1 With the **show cable hop history** command for entire CMTS, the most recent change of each action is displayed. 2 With the **show cable hop history** command for a MAC domain, the most recent three changes of each action are displayed. 3 With the **show cable hop history** command for a specific upstream, the last ten changes of each action are displayed. Changes are sorted by time with the most recent at the top. **Note** Supported in Cisco IOS Release 12.3(13a)BC or later release.
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*][**summary**	Displays hourly, daily, weekly, 30 days running average, and average since the system was brought up for each specified upstream. **Note** Supported in Cisco IOS Release 12.3(13a)BC or later release.
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*] **[history]**	

Command	Purpose
	Displays changes from one state to another, at any time and for any reason, for frequency, modulation, and channel width. **Note** Supported in Cisco IOS Release 12.3(23)BC7 or later release. The output of the **show cable hop history** is modified to include more information in the "change from" and "change to" fields of the output. Now, the modulation profile number is displayed when a change occurs, instead of the modulation order.
`Router# show cable modem [ip-address | interface | mac-address] [options]`	Displays information, including MER (SNR) values, for the registered and unregistered cable modems. **Note** Cisco IOS Release 12.3(13a)BC supports a **cnr** option that displays the CNR (CNiR) value for a specific cable modem, if it is using an upstream on the Cisco uBR10-MC5X20S/U/H BPE line card.
`Router# show cable modulation-profile [num] [initial | long | reqdata | request | short | station]`	Displays the configuration for all modulation profiles, for a particular modulation profile, or for a specific burst type for a particular modulation profile.
`Router# show cable spectrum-group[groupnum] [detail]`	Displays information about the spectrum groups that have been configured. **Note** The **detail** keyword is supported only in Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases.
`Router# show controllers cable x/y upstream n [ip-address | mac-address] start-freq end-freq res-freq`	Displays the upstream status, including the current frequency, channel width, modulation rate, and spectrum groups.
`Router# show controllers cable x/y upstream n spectrum [ip-address | mac-address] start-freq end-freq res-freq`	Displays the noise levels for a particular cable modem or displays the background noise for an entire upstream.

Note The **show cable flap-list** command displays the flap list of the CMTS router, which provides additional information about whether cable modems on an upstream are experiencing problems, and if so, what type of problems are occurring. For more information about the cable modem flapping and how to monitor the cable modem flap list, see the Flap List Troubleshooting for the Cisco CMTS Routers .

Using SNMP

You can use SNMP to monitor the spectrum management activity. The SNMP manager can be a graphically-based SNMP manager such as CiscoView or the Cable Broadband Troubleshooter (Release 3.0 or later).

The CISCO-CABLE-SPECTRUM-MIB has been enhanced to provide this SNMP support using the following MIB attributes:

ccsSNRRequestTable

The table below lists the attributes in the ccsSNRRequestTable table, which contains the CNR (CNiR) measurements that are made for individual cable modems on an upstream.

Table 62: ccsSNRRequestTable Attributes

Attribute	Type	Description
ccsSNRRequestIndex	Integer32	Arbitrary index to uniquely identify each table entry.
ccsSNRRequestMacAddr	MacAddress	MAC address of the remote online cable modem being reported on.
ccsSNRRequestSNR	Integer32	MER (SNR) value, in dB, that has been measured. This value is 0 when the Operation State is “running.”
ccsSNRRequestOperation	CCSRequestOperation	Sets the current operation: start, pending, running, or abort.
ccsSNRRequestOperState	CCSRequestOperState	Reports on the current operation state: idle, pending, running, noError, aborted, notOnLine, invalidMac, timeOut, fftBusy, fftFailed, others.
ccsSNRRequestStartTime	TimeStamp	Contains the time when the MER (SNR) measurement operation starts.
ccsSNRRequestStoppedTime	TimeStamp	Contains the time when the MER (SNR) measurement stops.
ccsSNRRequestStatus	RowStatus	Controls the modification, creation, and deletion of table entries.

ccsSpectrumRequestTable

The table below lists the attributes for each entry in the ccsSpectrumRequestTable table, which is used to obtain the spectrum profile for a particular cable modem or to obtain the background MER (SNR) for an entire upstream.

Table 63: ccsSpectrumRequestTable Attributes

Attribute	Type	Description
ccsSpectrumRequestIndex	Integer32	Arbitrary index to uniquely identify each table entry.
ccsSpectrumRequestIfIndex	InterfaceIndexOrZero	Interface identifying the upstream.
ccsSpectrumRequestMacAddr	MacAddress	MAC address to specify an MER (SNR) value for a particular cable modem, or 0000.0000.0000 to indicate background noise for the entire spectrum.
ccsSpectrumRequestUpperFreq	CCSFrequency	Upper frequency for the frequency range to be monitored (5000 to 42000 KHz, with a default of 42000 KHz).
ccsSpectrumRequestLowFreq	CCSFrequency	Lower frequency (in KHz) for the frequency range to be monitored (5000 to 42000 KHz, with a default of 5000 KHz).
ccsSpectrumRequestResolution	Integer32	Requested resolution to determine how the frequency range should be sampled (12 to 37000 KHz, with a default of 60 KHz).
ccsSpectrumRequestStartTime	TimeStamp	Time when the spectrum measurement began.
ccsSpectrumRequestStoppedTime	TimeStamp	Time when the spectrum measurement finished.
ccsSpectrumRequestOperation	CCSRequestOperation	Starts a new spectrum management request or aborts the current one.
ccsSpectrumRequestOperState	CCSRequestOperState	Provides the operational state of the current spectrum management request.
ccsSpectrumRequestStatus	RowStatus	Controls the modification, creation, and deletion of table entries.

ccsSpectrumDataTable

The table below lists the attributes in each entry of the ccsSpectrumDataTable table, which contains the results for a spectrum request.

Table 64: ccsSpectrumDataTable Attributes

Attribute	Type	Description
ccsSpectrumDataFreq	CCSMeasuredFrequency	Frequency in KHz for which this power measurement was made.
ccsSpectrumDataPower	INTEGER	Measured received power for the given frequency (–50 to 50 dBmV).

Note The ccsSpectrumRequestTable and ccsSpectrumDataTable tables provide the same information as that provided by the **show controllers cable upstream spectrum** command. This command is obsolete in Cisco IOS Release 12.3(21)BC.

ccsUpSpecMgmtTable

The table below lists the attributes in the ccsUpSpecMgmtTable table, which provides an entry describing each frequency hop.

Table 65: ccsUpSpecMgmtEntry Attributes

Attribute	Type	Description
ccsUpSpecMgmtHopPriority	INTEGER	Specifies the priority of frequency, modulation profile, and channel width in determining corrective action for excessive noise on the upstream (default is frequency, modulation profile, and channel width).
ccsUpSpecMgmtSnrThres1	Integer32	Specifies the upper MER (SNR) threshold for modulation profile 1 (5 to 35 dB, default of 25).
ccsUpSpecMgmtSnrThres2	Integer32	Specifies the upper MER (SNR) threshold for modulation profile 2 (5 to 35 dB, default of 13, and must be lower than that specified for ccsUpSpecMgmtSnrThres1).

Attribute	Type	Description
ccsUpSpecMgmtFecCorrectThres1	Integer32	Specifies the FEC correctable error threshold for modulation profile 1 (1 to 20 percent)
ccsUpSpecMgmtFecCorrectThres2	Integer32	Deprecated and no longer used.
ccsUpSpecMgmtFecUnCorrectThres1	Integer32	Specifies the FEC uncorrectable error threshold for modulation profile 1 (1 to 20 percent).
ccsUpSpecMgmtFecUnCorrectThres2	Integer32	Deprecated and no longer used.
ccsUpSpecMgmtSnrPollPeriod	Integer32	Deprecated and no longer used.
ccsUpSpecMgmtHopCondition	INTEGER	Reports the condition that triggers a frequency hop (MER [SNR] value or percentage of modems going offline).
ccsUpSpecMgmtFromCenterFreq	CCSFrequency	Provides the center frequency (in KHz) before the latest frequency hop.
ccsUpSpecMgmtToCenterFreq	CCSFrequency	Provides the current center frequency (in KHz) after the latest frequency hop.
ccsUpSpecMgmtFromBandWidth	CCSFrequency	Provides the channel width (in KHz) before the latest frequency hop.
ccsUpSpecMgmtToBandWidth	CCSFrequency	Provides the current channel width (in KHz) after the latest frequency hop.
ccsUpSpecMgmtFromModProfile	Integer32	Provides the modulation profile number before the latest frequency hop.
ccsUpSpecMgmtToModProfile	Integer32	Provides the current modulation profile number after the latest frequency hop.
ccsUpSpecMgmtSNR	Integer32	Provides the current MER (SNR) value (in dB) for the upstream.
ccsUpSpecMgmtCnrThres1	Integer32	Specifies the upper CNR (CNiR) threshold for modulation profile 1 (5 to 35 dB, default of 25).

Attribute	Type	Description
ccsUpSpecMgmtCnrThres2	Integer32	Specifies the upper CNR (CNiR) threshold for modulation profile 2 (5 to 35 dB, default of 13, and must be lower than that specified for ccsUpSpecMgmtCnrThres1).
ccsUpSpecMgmtCNR	Integer32	Provides the current CNR (CNiR) value (in dB) for the upstream.
ccsUpSpecMgmtMissedMaintMsgThres	Integer32	Provides the frequency hop threshold, as a percentage of station maintenance messages that are lost for a spectrum group.
ccsUpSpecMgmtHopPeriod	Integer32	Provide the minimum time, in seconds, between frequency hops.

ccsHoppingNotification

The table below describes the attributes contained in the notification that is sent after each frequency hop.

Table 66: ccsHoppingNotification Attributes

Attribute	Type	Description
ccsUpSpecMgmtHopCondition	INTEGER	Reports the condition that triggers a frequency hop (MER [SNR] value or percentage of modems going offline).
ccsUpSpecMgmtFromCenterFreq	CCSFrequency	Provides the center frequency (in KHz) before the latest frequency hop.
ccsUpSpecMgmtToCenterFreq	CCSFrequency	Provides the current center frequency (in KHz) after the latest frequency hop.
ccsUpSpecMgmtFromBandWidth	CCSFrequency	Provides the channel width (in KHz) before the latest frequency hop.
ccsUpSpecMgmtToBandWidth	CCSFrequency	Provides the current channel width (in KHz) after the latest frequency hop.

Attribute	Type	Description
ccsUpSpecMgmtFromModProfile	Integer32	Provides the modulation profile number before the latest frequency hop.
ccsUpSpecMgmtToModProfile	Integer32	Provides the current modulation profile number after the latest frequency hop.

Configuration Examples

This section provides the following configuration examples:

Spectrum Group and Combiner Group Examples

The following examples help you to determine whether spectrum group and combiner groups are configured and activated.

Example: Verifying Spectrum Group Creation

To verify that a spectrum group has been created, enter the **show cable spectrum-group** command:

```
Router# show cable spectrum-group
spectrum-group 1
spectrum-group 2
spectrum-group 3
```

Example: Time-Scheduled Spectrum Group

If your cable plant has an upstream noise characteristic on a weekly cycle, use time-scheduled spectrum allocation.

```
Router(config)# cable spectrum-group 1 time Mon 08:00:00 frequency 21600000
```

Deletion is performed using the **delete** keyword:

```
Router(config)# cable spectrum-group 1 time Mon 18:00:00 delete frequency 21600000
```

Example: Verifying Spectrum Group Configuration

To verify if spectrum groups have been configured and activated, enter the **show cable spectrum-group** command. This command displays each spectrum group, the frequencies assigned to it, the upstream port to which it has been assigned, whether a schedule exists for it, the currently measured power level, and whether it is a shared spectrum group.

```
Router# show cable spectrum-group

22:07:46: %SYS-5-CONFIG_I: Configured from console by console
Group  Frequency      Upstream     Weekly Scheduled            Power   Shared
No.    Band           Port         Availability                Level   Spectrum
       (Mhz)                       From Time:    To Time:      (dBmV)
1       5.000-15.000                                           0       Yes
1      12.000                                                  0       Yes
```

```
1      22.000         Cable6/0 U5                              7       Yes
2      29.000         Cable6/0 U4                              6       No
2      26.000                                                  0       No
3      35.000-41.000                                           0       No
3      16.000-19.000  Cable6/0 U3                              5       No
5*      5.000-10.000              Thu 21:50:00  Thu 21:45:00  0       Yes
```

Example: Determining the Upstream Ports Assigned to a Combiner Group

Following is a sample topology for a CMTS with combiner groups designated A through J. Combiner groups C and E have multiple upstream ports that should be configured in a shared spectrum group. The other upstreams should be configured in a nonshared spectrum group.

In this example, ten combiner groups are served with frequency hop tables from three spectrum groups:

```
Cable3/0
DS +-----+ Upconverter +----- laser group 1
U0 +----- combiner group A
U1 +----- combiner group B
U2 +------combiner group C
U3 +------combiner group C
U4 +----- combiner group D
U5 +------combiner group E
Cable4/0
DS +-----+ Upconverter +----- laser group 2
U0 +------combiner group E
U1 +----- combiner group F
U2 +----- combiner group G
U3 +----- combiner group H
U4 +----- combiner group I
U5 +----- combiner group J
```

The *laser group* term refers to the set of fiber nodes that share the same downstream signal. An optical splitter is often used to create individual feeds per node.

In the downstream direction, two 6-MHz channel slots are assigned. All fiber nodes in combiner groups A through E should have a channel slot containing the downstream signal from Cable3/0. Combiner groups A through E are said to belong to laser group 1.

All fiber nodes in combiner groups E through J should have a channel slot containing the downstream signal from Cable4/0. Combiner groups E through J are said to belong to laser group 2.

Because combiner group E belongs to two laser groups, there should be two different downstream channel slots for Cable3/0 and Cable4/0.

Example: Combiner Group

The following example enables spectrum management for all upstream ports, where all combiner groups use the frequency band from 20 to 26 MHz:

```
CMTS01(config)# cable spectrum-group 1 band 20000000 26000000
CMTS01(config)# cable spectrum-group 2 shared
CMTS01(config)# cable spectrum-group 2 band 20000000 26000000
CMTS01(config)# cable spectrum-group 3 shared
CMTS01(config)# cable spectrum-group 3 band 20000000 26000000
CMTS01(config)# interface Cable3/0
CMTS01(config-if)# cable spectrum-group 1
CMTS01(config-if)# cable upstream 2 spectrum-group 2
CMTS01(config-if)# cable upstream 3 spectrum-group 2
CMTS01(config-if)# cable upstream 5 spectrum-group 3
CMTS01(config-if)# exit
CMTS01(config)# interface Cable4/0
CMTS01(config-if)# cable spectrum-group 1
CMTS01(config-if)# cable upstream 0 spectrum-group 3
```

A description of the spectrum groups 1 through 3 follows:

- Spectrum group 1—This group is nonshared. Upstream RF domains exist for each member upstream port.

```
Upstream Port   RF Domain
Cable3/0 U0     combiner group A
Cable3/0 U1     combiner group B
Cable3/0 U4     combiner group D
Cable4/0 U1     combiner group F
Cable4/0 U2     combiner group G
Cable4/0 U3     combiner group H
Cable4/0 U4     combiner group I
Cable4/0 U5     combiner group J
```

- Spectrum group 2—This group is shared. A single upstream RF domain exists.

```
Upstream Port   RF Domain
Cable3/0 U2     combiner group C
Cable3/0 U3     combiner group C
```

- Spectrum group 3—This group is shared. A single upstream RF domain exists.

```
Upstream Port   RF Domain
Cable3/0 U5     combiner group E
Cable4/0 U0     combiner group E
```

For the 20- to 26-MHz band of each RF domain, the spectrum is channelized according to the channel width settings of each member port. For example, if the ports U2 and U3 of Cable3/0 are set to 3.2 MHz and 1.6 MHz channel widths, respectively, then spectrum group 2 uses the following channelization:

```
> Channel Width Start Stop Center
>           (Mhz) (Mhz) (Mhz) (Mhz)
> 1         3.2    20.0 23.2 21.6
> 2*        1.6    20.0 21.6 20.8
> 3*        1.6    21.6 23.2 22.4
> 4         1.6    23.2 24.8 24.0
```

Note Channels 2 and 3 are not available when channel 1 is in use.

Because the group is shared, ports U2 and U3 will be assigned channels 1 and 4, respectively, to prevent overlap.

Note There are no alternate frequency assignments for either port, and bandwidth is wasted from 24.8 to 26.0 MHz. To create alternate channels, increase the upper boundary from 26.0 to 28.0 MHz.

```
> Channel  Width  Start Stop  Center
>           (Mhz)  (Mhz) (Mhz) (Mhz)
>  1         3.2    20.0  23.2  21.6
>  2         3.2    23.2  26.4  24.8
>  3         1.6    20.0  21.6  20.8
>  4         1.6    21.6  23.2  22.4
>  5         1.6    23.2  24.8  24.0
>  6         1.6    24.8  26.4  25.6
>  7         1.6    26.4  28.0  27.4
```

Try to reduce the spectrum allocation when it is used with small channel widths. Otherwise, there will be a large number of upstream channel slots, and the frequency hopping may require several minutes to find a clean slot.

Example: Other Spectrum Management Configurations

To configure differing spectrum groups, refer to the following examples:

- Use the following example to add a time-scheduled spectrum. You can add a spectrum on a weekly schedule by including an optional weekday and time:

```
Router(config)# cable spectrum-group 1 time Mon 08:00:00 frequency 21600000
```

- Use the **delete** keyword to delete the frequency:

```
Router(config)# cable spectrum-group 1 time Mon 18:00:00 delete frequency 21600000
```

- Use the following example to configure spectrum group 1 with an upstream frequency of 6,500,000 Hz and a default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 1 frequency 6500000
```

- Use the following example to add the upstream frequency 7,000,000 Hz to the list of valid frequencies with a default power level of 0 dBmV for spectrum group 1:

```
Router(config)# cable spectrum-group 1 frequency 7000000
```

- Use the following example to configure spectrum group 2 with an upstream frequency 7,500,000 Hz and change the power level to 5 dBmV:

```
Router(config)# cable spectrum-group 2 frequency 7500000 5
```

- Use the following example to configure spectrum group 3 with an upstream band of 12,000,000 to 18,000,000 Hz and default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 3 band 12000000 18000000
```

- Use the following example to add the upstream band 20,000,000 to 24,000,000 Hz to the list of valid bands with a change in the power level of 13 dBmV for spectrum group 3:

```
Router(config)# cable spectrum-group 3 band 20000000 24000000 13
```

- Use the following example to configure a continuous band between 5,000,004 and 40,000,000 Hz for scheduled spectrum group 4 with a default power level of 0 dBmV. The band is available to the spectrum group starting at 12:00 p.m. local time each Monday:

```
Router(config)# cable spectrum-group 4 time Monday 12:00:00 band 5000004 40000000
```

- Use the following example to add the upstream frequency 9,500,000 Hz to the list of valid frequencies and change the nominal power level to 5 dBmV. The spectrum manager adjusts frequencies and power levels on this group at 2:00 a.m. local time each day:

```
Router(config)# cable spectrum-group 3 time 02:00:00 frequency 9500000 5
```

- Use the following example to configure the minimum period before which a frequency hop can occur in seconds:

```
Router(config)# cable spectrum-group 3 hop period 800
```

- Use the following example to configure the threshold value (expressed as a percentage) of the number of “offline” modems identified before the router initiates an automatic frequency hop:

```
Router(config)# cable spectrum-group 3 hop threshold 40
```

- Use the following example to configure a particular spectrum group as a shared RF spectrum group. Specifying a given spectrum group as “shared” tells the router that you want to be sure that upstream frequencies assigned to upstream ports are not assigned to additional upstream ports:

```
Router(config)# cable spectrum-group 3 shared
```

- Use the following example to remove a specified spectrum group from your configuration:

```
Router(config)# no cable spectrum-group 3
```

- The following is an example of a spectrum group configuration that is designed to perform minor equalization as a function of frequency.

```
Router(config)# cable spectrum-group 1 frequency 21600000
Router(config)# cable spectrum-group 1 frequency 24800000 1
Router(config)# cable spectrum-group 1 frequency 28000000 2
```

  In this example, the upstream port receives power at 21.6 MHz with a default power level of 0 dBmV, at 24.8 MHz with a power level of 1 dBmV, and at 28.0 MHz with a power level of 2 dBmV. At any time, the power level set in the interface configuration overrides the spectrum group power level.

Dynamic Upstream Modulation Examples

The following examples describe how to display modulation profile information with the **show cable modulation-profile** command and to define a modulation profile with the **cable modulation-profile** command.

Verifying Your Settings

Step 1 To check the value of the settings you have entered, enter the **show running-config** command in privileged EXEC mode:

Example:

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

To review changes you make to the configuration, use the **show startup-config** command in privileged EXEC mode to display the information stored in NVRAM.

Step 2 To display modulation profile group information, use the **show cable modulation-profile** command in privileged EXEC mode:

Example:

```
Router# show cable modulation-profile[profile][iuc-code]
```

This command uses the following syntax:

- *profile*—(Optional) Profile number. Valid values are from 1 to 8.
- *iuc-code*—(Optional) Internal usage code.

Valid options are:

- **initial—**Initial ranging burst
- **long—**Long grant burst
- **request—**Request burst
- **short—**Short grant burst
- **station—**Station ranging burst

Example: Modulation Profiles

In Cisco IOS Release 12.1(3a)EC1 and later, the Cisco CMTS has one preconfigured modulation profile resident in memory, which defines a typical profile for QPSK modulation. 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, more robust modulation scheme.

The following example is a modulation profile for QAM-16, in which the initial, request, and station maintenance messages are sent as QPSK, and the short and long data packets are sent as QAM-16. The QAM-16 modulation is more bandwidth-efficient than QPSK, but QPSK is more robust than QAM-16.

Note The upstream request and station maintenance messages use less time on the cable network when configured in QPSK for symbol rates of 640K, 1280K, and 2560K symbols/sec. Thus, these messages are actually more efficient when used in QPSK mode and they ensure a more reliable modem connection. The upstream initial maintenance message takes exactly the same amount of time on the cable network, no matter how it is configured. Modems connect more quickly and experience fewer cycles of power adjustment during initial maintenance if the system is set for QPSK.

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 qpsk scrambler 152 no-diff 64
fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 72
fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

In the following example, all message types are carried with QAM-16 modulation. Although QAM-16 modulation offers a consistent modulation scheme for all five types of messages, the added length of the QAM-16 preamble offsets the increased bandwidth efficiency of the MAC data message for the station maintenance messages and bandwidth request messages.

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 16qam scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 16qam scrambler 152 no-diff
256 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 16qam scrambler 152 no-diff
```

```
256 fixed uw16
Router(config)# cable modulation-profile 2 short 5 75 6 8 16qam scrambler 152 no-diff 144
fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

Note When using DOCSIS concatenation with a 16-QAM or mixed symbol rate, configure the CMTS for Unique Word 16 ("uw16") in the preamble for both short and long data burst profiles.

Add the **cable upstream** *port-number* **modulation-profile** *primary profile-number secondary profile-number* command to the appropriate interfaces. In this example, modulation profile 2 is for QAM-16 modulation and profile 1 is for QPSK modulation.

```
Router# configure terminal
Router(config)# interface Cable6/0
Router(config-if)# cable upstream 0 modulation-profile 2 1
```

Example: Input Power Level

In the following example, the modem transmit power at 24.8 MHz is adjusted upstream by 1 dBmV and the modem transmit power at 28.0 MHz is adjusted upstream by 2 dBmV.

```
CMTS01(config)# cable spectrum-group 1 frequency 21600000
CMTS01(config)# cable spectrum-group 1 frequency 24800000 1
CMTS01(config)# cable spectrum-group 1 frequency 28000000 2
```

Advanced Spectrum Management Configuration Examples

This section provides the following typical configurations:

Example: Advanced Spectrum Management for the Cisco uBR7200 Series Router

This section provides a typical configuration example for a Cisco uBR7200 series router using the Cisco uBR-MC16U cable interface line card. This configuration does the following:

- Creates three spectrum groups with different frequency bands, hop periods, and hop thresholds.
- Creates two upstream modulation profiles, one for QPSK operation and one for QAM-16 operation, by specifying the parameters for each burst type.
- Creates two upstream modulation profiles, one for QPSK operation and one for mixed QPSK/QAM-16 operation, using the default profile options (**qpsk** and **mix**).
- Configures one upstream (port 5) on cable interface 3/0 to use spectrum group 3.
- Configures the upstreams with the primary modulation profile set to mixed QPSK/QAM-16 operation and the secondary modulation profile set for QPSK operation.
- Configures the upstream so that when its noise threshold is reached, it first attempts to change the frequency, then the channel-width, and finally to switch the modulation profile (using the Dynamic Upstream Modulation feature).

```
!
```

```
version 12.3
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ubr7200
!
!
! Define a frequency band for a 1.6 MHz channel around center frequency of 20.800 MHz
cable spectrum-group 1 band 19750000 21850000 0
! Define a frequency band for a 1.6 MHz channel around center frequency of 23.200 MHz
cable spectrum-group 1 band 22150000 24250000 0
! Hop period set to 30 sec to avoid modems going offline before initiating a hop priority
cable spectrum-group 1 hop period 30
! Percentage of missed station maintenance from modems
cable spectrum-group 1 hop threshold 20
!
cable modulation-profile 1 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
! Create second modulation profile numbered 4
cable modulation-profile 4 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 4 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 4 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16
! Create two modulation profiles using the default QPSK and QPSK/16-QAM profiles
cable modulation-profile 3 qpsk
cable modulation-profile 5 mix
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
clock calendar-valid
no ip subnet-zero
no ip domain-lookup
!
!
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 shutdown
 media-type MII
 full-duplex
!
interface Ethernet1/0
 ip address 10.11.10.1 255.0.0.0
 no ip mroute-cache
 half-duplex
!
interface Cable3/0
 ip address  255.255.255.0 secondary
 ip address  255.255.255.0
 no keepalive
 cable map-advance static
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 687000000
! Assign upstream to spectrum group
 cable upstream 0 spectrum-group 1
! Set channel-width to be fixed at 1.6 MHz
 cable upstream 0 channel-width 1600000 1600000
! Set priority of corrective actions
 cable upstream 0 hop-priority frequency channel-width modulation
! Set the thresholds for corrective action
cable upstream 0 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
! Assign modulation profiles to upstream port in order of preference
```

```
 cable upstream 0 modulation-profile 5 1
 no cable upstream 0 concatenation
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 1
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 hop-priority frequency channel-width modulation
cable upstream 1 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 1 modulation-profile 5 1
 no cable upstream 1 concatenation
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 1
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 hop-priority frequency channel-width modulation
cable upstream 2 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 2 modulation-profile 5 1
 no cable upstream 2 concatenation
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 1
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 hop-priority frequency channel-width modulation
cable upstream 3 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 3 modulation-profile 5 1
 no cable upstream 3 concatenation
 no cable upstream 3 shutdown
 cable upstream 4 spectrum-group 1
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 hop-priority frequency channel-width modulation
cable upstream 4 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 4 modulation-profile 5 1
 no cable upstream 4 concatenation
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 1
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 5 modulation-profile 5 1
 no cable upstream 5 concatenation
 no cable upstream 5 shutdown
 no cable dci-response
 cable dhcp-giaddr policy
!
interface Cable4/0
 no ip address
 no keepalive
 cable map-advance static
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 687000000
 cable upstream 0 spectrum-group 1
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 0 modulation-profile 5 1
 no cable upstream 0 concatenation
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 1
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
```

```
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 1 modulation-profile 5 1
 no cable upstream 1 concatenation
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 1
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 2 modulation-profile 5 1
 no cable upstream 2 concatenation
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 1
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 3 modulation-profile 5 1
 no cable upstream 3 concatenation
 no cable upstream 3 shutdown
 cable upstream 4 spectrum-group 1
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 4 threshold Uncorr-Fec 2
 cable upstream 4 modulation-profile 5 1
 no cable upstream 4 concatenation
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 1
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profiles 23 15
cable upstream 0 threshold Corr-Fec 5
cable upstream 0 threshold Uncorr-Fec 2
 cable upstream 5 modulation-profile 5 1
 no cable upstream 5 concatenation
 no cable upstream 5 shutdown
 no cable dci-response
 cable dhcp-giaddr primary
!
ip default-gateway 10.11.0.1
ip classless
ip route 10.11.254.254 255.255.255.255 10.11.0.1
no ip http server
!!
snmp-server engineID local 00000009020000D0CAA7BB00
snmp-server community private RW
snmp-server trap-source FastEthernet0/0
snmp-server packetsize 2048
snmp-server system-shutdown
snmp-server enable traps cable hopping
snmp-server manager
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 no login
!
end
```

Example: Advanced Spectrum Management for the Cisco uBR10012 Router

This section provides an excerpt from a typical configuration example for a Cisco uBR10012 router using the Cisco uBR10-MC5X20S/U/H cable interface line card. This configuration does the following:

- Configures four spectrum groups with a hop period of 30 seconds.
- Creates a QPSK modulation profile and assigns it to four upstreams on the Cisco uBR-MC5X20S/U/H cable interface line card in slot 6/1/0.
- Assigns a spectrum group to each of the four upstreams.
- Configures each upstream for the default CNR (CNiR) and FEC thresholds.

```
cable modulation-profile 21 qpsk
interface Cable6/1/0
cable bundle 1
cable downstream annex B
cable downstream modulation 256qam
cable downstream interleave-depth 32
! upstream 0
cable upstream 0 spectrum-group 1
cable upstream 0 modulation-profile 21
cable upstream 0 threshold cnr-profiles 16 0
cable upstream 0 threshold Corr-Fec 3
cable upstream 0 threshold Uncorr-Fec 1
no cable upstream 0 shutdown ! upstream 1
cable upstream 1 spectrum-group 2
cable upstream 1 modulation-profile 21
cable upstream 1 threshold cnr-profiles 16 0
cable upstream 1 threshold Corr-Fec 3
cable upstream 1 threshold Uncorr-Fec 1
no cable upstream 1 shutdown ! upstream 2
cable upstream 2 spectrum-group 3
cable upstream 2 modulation-profile 21
cable upstream 2 threshold cnr-profiles 16 0
cable upstream 2 threshold Corr-Fec 3
cable upstream 2 threshold Uncorr-Fec 1
no cable upstream 2 shutdown ! upstream 3
cable upstream 3 spectrum-group 4
cable upstream 3 modulation-profile 21
cable upstream 3 threshold cnr-profiles 16 0
cable upstream 3 threshold Corr-Fec 3
cable upstream 3 threshold Uncorr-Fec 1
no cable upstream 3 shutdown
```

Additional References

The following sections provide references related to Spectrum Management and Advanced Spectrum Management for the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
CMTS Command Reference	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html Cisco Broadband Cable Command Reference Guide.

Related Topic	Document Title
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Cable Features Configuration Guide	Cisco CMTS Feature Guide
Installing Cisco uBR7100 Series Universal Broadband Routers	Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide
Configuring Cisco uBR7100 Series Universal Broadband Routers	Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide
Installing Cisco uBR7200 Series Universal Broadband Routers	Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide Cisco uBR7200 Series Universal Broadband Router Cable Modem Card Installation and Configuration Cisco uBR7200 Series Universal Broadband Router Port Adapter Installation and Configuration Cisco uBR7200 Series Universal Broadband Router 550-Watt DC-Input Power Supply Replacement Instructions Cisco uBR7200 Series Universal Broadband Router Subchassis and Midplane Replacement Instructions Cisco uBR7200 Series Rack-Mount and Cable-Management Kit Installation Instructions Cisco uBR7200 Series Universal Broadband Router Fan Tray Replacement Instructions
Configuring Cisco uBR7200 Series Universal Broadband Routers	Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide Cisco uBR7200 Series Universal Broadband Router Feature Roadmap

Related Topic	Document Title
Installing Cisco uBR10012 Universal Broadband Routers	Cisco uBR10012 Series Universal Broadband Router Hardware Installation Guide 2400W AC-Input Power Shelf for the Cisco uBR10012 Series Universal Broadband Router Cable Interface Line Card Processor Hardware Installation for the Cisco uBR10012 Series Universal Broadband Router Fan Assembly Module for the Cisco uBR10012 Series Universal Broadband Router DC Power Entry Module for the Cisco uBR10012 Series Universal Broadband Router Performance Routing Engine Card Hardware Installation for the Cisco uBR10012 Series Universal Broadband Router TCC+ Card for the Cisco uBR10012 Series Universal Broadband Router
Configuring the Cisco uBR10012 Universal Broadband Routers	Cisco uBR10012 Universal Broadband Router Software Configuration Guide

Standards and RFCs

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0

MIBs

MIBs	MIBs Link
CISCO-CABLE-SPECTRUM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Spectrum Management and Advanced Spectrum Management on CMTS

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 67: Feature Information for Spectrum Management

Feature Name	Releases	Feature Information
Spectrum Management	11.3(9)NA, 12.0(6)SC, and 12.1(2)EC	Guided and scheduled spectrum management was introduced on Cisco uBR7200 series universal broadband routers.

Feature Name	Releases	Feature Information
Spectrum Management	12.1(5)EC	Support was added for guided and scheduled spectrum management on Cisco uBR7100 series universal broadband routers.
Spectrum Management	12.1(10)EC1 and 12.2(4)BC1	The MER (SNR) algorithm was corrected to display a more accurate value for upstreams.
Spectrum Management	12.2(4)BC1	Support was added for guided and scheduled spectrum management on Cisco uBR10012 routers.
Spectrum Management	12.2(15)BC1	Support was added for guided and scheduled spectrum management on the Cisco uBR10-MC5X20S/U/H cable interface line card.
Spectrum Management	12.2(15)BC2	This release added the following support: • Support was added for intelligent and advanced spectrum management on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards. • Support was added for guided and scheduled spectrum management on the Cisco uBR10-MC5X20S/U/H line card. • The maximum number of spectrum groups was increased from 32 to 40 groups per router. • The number of predefined modulation profiles was increased.

Feature Name	Releases	Feature Information
Cisco Broadband Troubleshooter (CBT)	12.3(9)BC	This release added the following support: • Spectrum management support with the Cisco Broadband Troubleshooter (CBT) 3.2 for the Cisco MC5X20S/U/H Broadband Processing Engine (BPE).
Advanced Spectrum Management	12.3(13a)BC	This release added the following support: • Advanced spectrum management support for the Cisco MC5X20S/U/H BPE in the Cisco uBR10012 Universal Broadband Router.
Spectrum Management	12.3(21)BC	This release added the following support: • Shared spectrum groups for DOCSIS 3.0, otherwise referred to as Fiber Node Groups, supporting inter-line card or intra-line card group combining. Refer to the Configuring Shared Spectrum Groups (Fiber Node Groups) for DOCSIS 3.0, on page 596. • The **show controllers cable upstream spectrum** command is obsolete.

Feature Name	Releases	Feature Information
Dynamic Upstream Modulation	12.3(23)BC7	The Dynamic Upstream Modulation feature was enhanced to support a configuration of up to three modulation profiles. 64-QAM-based modulation profile is used to increase the upstream throughput and to satisfy the demand for new spectrum management. The following commands were introduced or modified: • **cable upstream modulation** • **cable upstream threshold hysteresis** • **show cable hop history**
Three Step Dynamic Modulation	12.2(33)SCB3	This release added support for the Three Step Dynamic Modulation feature.
DOCSIS3.0 CNiR Measurement	12.2(33)SCF	This feature was added to support CNiR (CNR) measurement for all US channels irrespective of whether spectrum management feature is enabled or not on the US channels. The **show cable modem cnr** command was modified.

CHAPTER 24

Support for Extended Upstream Frequency Ranges

First Published: February 14, 2008

Cisco IOS Release 12.2(15)BC2 adds support for the extended upstream frequency range that is used in cable networks in Japan and other areas. This feature also clarifies the configuration of DOCSIS and EuroDOCSIS networks, so that the router shows only those upstream and downstream frequencies that are valid for each mode of operation.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Extended Upstream Frequency Ranges

- The Cisco CMTS router must be running Cisco IOS Release 12.2(15)BC2 or later releases.
- The North American upstream frequency range (DOCSIS, 5 MHz to 42 MHz) is supported on all Cisco CMTS routers and all cable interfaces.
- The European upstream frequency range (EuroDOCSIS, 5 MHz to 65 MHz) is supported on the following platforms and cable interfaces:
  - Cisco uBR7111E and Cisco uBR7114E routers
  - Cisco uBR7246VXR router with the Cisco uBR-MC16E, Cisco uBR-MC16U/X, or Cisco uBR-MC28U/X cable interface line cards.
  - Cisco uBR10012 router with the Cisco uBR-LCP2-MC16E or Cisco uBR-MC5X20U cable interface line cards.
- The Japanese extended upstream frequency range (5 MHz to 55 MHz) is supported on the following platforms and cable interfaces:
  - Cisco uBR7111E and Cisco uBR7114E routers
  - Cisco uBR7246VXR router with the Cisco uBR-MC16E, Cisco uBR-MC16U/X, or Cisco uBR-MC28U/X cable interface line cards.
  - Cisco uBR10012 router with the Cisco uBR-LCP2-MC16E or Cisco uBR-MC5X20U cable interface line cards.
- The cable physical plant must be configured with upconverters, filters, and other equipment that supports the desired frequency range and DOCSIS modes of operation.

Restrictions for Extended Upstream Frequency Ranges

- The RF modulation format should be configured for ITU J.112 Annex A for EuroDOCSIS operations, and for ITU J.83 Annex B for DOCSIS and Japanese operations. While it is possible to configure the modulation format differently, we do not recommend this because it violates the DOCSIS and EuroDOCSIS specifications.
- The ITU J.83 Annex C specification is not supported.
- You cannot configure the router for a particular frequency range if an upstream or spectrum group on the router is currently configured for a frequency that is invalid for the new range. If you try to do so, the command is ignored and a warning message is printed prompting you to reconfigure the upstream or spectrum group before retrying the command.

Information About Extended Upstream Frequency Ranges

The original Data-over-Cable Service Interface Specifications (DOCSIS) specified a range of downstream and upstream frequencies that were compatible only with the North American National Television Systems

Committee (NTSC) channel plans.Those specifications have been enhanced to provide support for other cable systems.

Frequency Ranges Currently in Use

The table below lists the specifications that are commonly used in cable plants at the current time:

Table 68: Frequency Specifications

Region	Channel Plan	Radio Frequency (RF)[42] Modulation Format	Downstream Frequency Range	Upstream Frequency Range
North American (DOCSIS)	6 MHz NTSC[43]	ITU J.83 Annex B	85 MHz to 860 MHz	5 MHz to 42 MHz
European (EuroDOCSIS)	8 MHz PAL[44]/SECAM[45]	ITU J.112 Annex A	85 MHz to 860 MHz	5 MHz to 65 MHz
Japan[46]	6 MHz NTSC	ITU J.83 Annex B	70 MHz to 860 MHz	5 MHz to 55 MHz

42 The RF Modulation Format column shows the configuration that is required for operation in normal DOCSIS and EuroDOCSIS networks. While it is possible to configure the Modulation Format differently than what is shown in this table, we do not recommend doing so.

43 NTSC = North American National Television Systems Committee

44 PAL = Phase Alternating Line

45 SECAM= Systeme Electronique Couleur Avec Memoire

46 CableLabs has not released an official version of the DOCSIS specification to support the extended Japanese upstream and downstream frequency ranges.

Extended Frequency Support for Downstreams

All current Cisco cable interface line cards support downstream frequencies between 54 MHz and 860 MHz, which is a superset of the DOCSIS and EuroDOCSIS downstream frequency range. This allows those cards to automatically support the extended downstream frequency range of Japanese networks, assuming that the appropriate upconverters, filters, and other supporting equipment is also installed in the cable plant.

Extended Frequency Support for Upstreams

To support the different upstream frequency ranges, Cisco IOS Release 12.2(15)BC2 introduces a new command, **cable freq-range** , which configures the Cisco CMTS router for the maximum allowable range of frequencies that can be used on the router. This command makes these frequencies available only for those cable interfaces that support them.

Tip The **cable freq-range** command is not normally needed except to enable EuroDOCSIS operations on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards. However, it can be used in other situations to ensure that the other **cable upstream** commands do not allow frequencies outside of the desired range.

Support for the different frequency ranges depends on the cable interfaces being used:

- Cisco uBR-MC16E cable interface line card and the Cisco uBR7111E/7114E routers—Support the EuroDOCSIS frequency range, which is the default mode of operation.

- Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20U cable interface line cards—Support the Japanese extended frequency range and the EuroDOCSIS frequency range, and the Japanese range is the default mode of operation.
- All other cable interfaces—Support the DOCSIS frequency range, which is the default mode of operation.

If a cable interface card does not support the frequency range that is configured with the **cable freq-range** command, a warning message is displayed. The card interface card, however, can continue to be used with its normal set of frequencies.

For example, consider the case where a Cisco uBR7246VXR router has a Cisco uBR-MC16C card and a Cisco uBR-MC28U card installed. By default, the Cisco uBR-MC16C card supports the DOCSIS frequency range, and the Cisco uBR-MC28U supports the Japanese frequency range. If you configure the router to support the EuroDOCSIS frequency range, only the Cisco uBR-MC28U card supports the extra downstream and upstream frequencies. The Cisco uBR-MC16C card, however, can continue to be used with the regular DOCSIS frequencies.

How to Configure the Upstream Frequency Range

To configure a Cisco CMTS router to use a particular range of upstream frequencies, use the following procedures:

Note You do not need any special configuration to be able to use the extended range of downstream frequencies that is used in Japanese networks, because all currently-supported Cisco cable interface line cards support a superset (54 MHz to 860 Mhz) of the DOCSIS frequencies that include the Japanese range.

Configuring DOCSIS Upstream Frequencies

To configure one or more upstreams with a frequency in the valid DOCSIS range of 5 MHz to 42 MHz, use the following procedure.

Tip This procedure typically is not needed, because by default all cable interfaces support the DOCSIS frequency range. However, you might want to use this procedure for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards to specify that these cards use a narrower DOCSIS frequency filter that would filter out any noise in the frequencies above 42 MHz, which might improve RF performance on some cable plants.

Before You Begin

All Cisco CMTS platforms and cable interfaces support the North American range of upstream frequencies.

Restriction All cable interfaces in the router must be using the North American upstream frequency range.

Any upstreams that are currently configured for frequencies greater than 42 MHz must be reconfigured to use a lower frequency, using the **cable upstream frequency** interface command, before beginning this procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable freq-range north-american** **Example:** `Router(config)# cable freq-range north-american`	Configures the Cisco CMTS router for the DOCSIS upstream frequency range (5 MHz to 42 MHz). **Note** This command will fail if any upstreams are currently configured with frequencies greater than 42 MHz. Use the **cable upstream frequency** command to reconfigure these upstreams for a lower frequency and then re-enter this command.
Step 4	**interface cable** {*x/y* | *x/y/z* } **Example:** `Router(config)# interface cable 3/0`	Enters interface cable configuration mode for the specified cable interface.
Step 5	**cable downstream annex b** **Example:** `Router(config-if)# cable downstream annex b`	Configures the downstream for the Annex B (ITU J.83) RF mode, which is used in DOCSIS networks.
Step 6	**cable upstream** *n* **frequency** *frequency* **Example:** `Router(config-if)# cable upstream 0 frequency 32000000`	Configures the upstream for the desired frequency in Hertz. The valid range for *n* starts with 0 and depends on the number of upstream ports for this downstream. The valid range for *frequency* is 5000000 to 42000000. **Note** Repeat this command for each upstream port for this downstream.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Extended DOCSIS Upstream Frequencies for Japan

To configure one or more upstreams with a frequency in the extended Japanese frequency range of 5 MHz to 55 MHz, use the following procedure.

Note This procedure is not typically needed, because all of the cable interfaces listed in the Before You Begin section support the extended upstream frequency ranges in their default configuration. However, if you have configured a Cisco uBR-MC16U/X or Cisco uBR-MC28U/X card as described in the Configuring DOCSIS Upstream Frequencies, on page 642, you must use this procedure to re-enable the extended frequency range.

Before You Begin

The Japanese upstream frequency range (5 MHz to 55 MHz) is supported on the following platforms and cable interfaces:

- Cisco uBR7111E and Cisco uBR7114E routers
- Cisco uBR7246VXR router with the Cisco uBR-MC16E, Cisco uBR-MC16U/X, or Cisco uBR-MC28U/X cable interface line cards.
- Cisco uBR10012 router with the Cisco uBR-LCP2-MC16E or Cisco uBR-MC5X20U cable interface line cards.

Restriction All cable interfaces in the router must be using either the North American or the Japanese upstream frequency range.

Any upstream that is currently configured for EuroDOCSIS, using frequencies greater than 55 MHz must be reconfigured for a lower frequency, using the **cable upstream frequency** interface command, before beginning this procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable freq-range japanese** **Example:** `Router(config)# cable freq-range japanese`	Configures the Cisco CMTS router for the extended upstream frequency range (5 MHz to 55 MHz) that is used in Japanese cable networks.

	Command or Action	Purpose
		Note This command will fail if any upstreams are currently configured with frequencies greater than 55 MHz. Use the **cable upstream frequency** command to reconfigure these upstreams for a lower frequency and then re-enter this command.
Step 4	**interface cable** {*x/y* | *x/y/z* } **Example:** `Router(config)# interface cable 3/0`	Enters interface cable configuration mode for the specified cable interface.
Step 5	**cable downstream annex b** **Example:** `Router(config-if)# cable downstream annex b`	Configures the downstream for the Annex B (ITU J.83) RF mode, which is used in DOCSIS networks.
Step 6	**cable upstream** *n* **frequency** *frequency* **Example:** `Router(config-if)# cable upstream 0 frequency 32000000`	Configures the upstream for the desired frequency in Hertz. The valid range for *n* starts with 0 and depends on the number of upstream ports for this downstream. The valid range for *frequency* is 5000000 to 55000000. **Note** Repeat this command for each upstream port for this downstream.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring EuroDOCSIS Upstream Frequencies

To configure one or more upstreams with a frequency in the valid EuroDOCSIS range of 5 MHz to 65 MHz, use the following procedure.

Tip This command is not normally needed with the Cisco UBR-MC5X20U cable interface line card, because by default it supports upstream frequencies up to 65 MHz. However, if you have used one of the previous procedures, Configuring DOCSIS Upstream Frequencies, on page 642 or Configuring Extended DOCSIS Upstream Frequencies for Japan, on page 644, to limit the frequency range, you must use this procedure to re-enable the EuroDOCSIS frequency range.

Before You Begin

The European upstream frequency range (EuroDOCSIS, 5 MHz to 65 MHz) is supported on the following platforms and cable interfaces:

- Cisco uBR7111E and Cisco uBR7114E routers
- Cisco uBR7246VXR router with the Cisco uBR-MC16E, Cisco uBR-MC16U/X, or Cisco uBR-MC28U/X cable interface line cards.
- Cisco uBR10012 router with the Cisco uBR-LCP2-MC16E or Cisco uBR-MC5X20U cable interface line cards.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable freq-range european** **Example:** `Router(config)# cable freq-range european`	Configures the Cisco CMTS router for the EuroDOCSIS upstream frequency range (5 MHz to 65 MHz).
Step 4	**interface cable** {*x/y* | *x/y/z* } **Example:** `Router(config)# interface cable 3/0`	Enters interface cable configuration mode for the specified cable interface.
Step 5	**cable downstream annex a** **Example:** `Router(config-if)# cable downstream annex a`	Configures the downstream for the Annex A (ITU J.112) RF mode, which is used in EuroDOCSIS networks. **Note** You must configure the downstream for Annex A for EuroDOCSIS operations. You can configure certain cable interface cards (such as the Cisco uBR-MC28U) for both Annex B (DOCSIS) and the EuroDOCSIS frequency range, but this violates the DOCSIS specifications and should not be used on standard DOCSIS networks.
Step 6	**cable upstream** *n* **frequency** *frequency* **Example:** `Router(config-if)# cable upstream 0 frequency 32000000`	Configures the upstream for the desired frequency in Hertz. The valid range for *n* starts with 0 and depends on the number of upstream ports for this downstream. The valid range for *frequency* is 5000000 to 65000000. **Note** Repeat this command for each upstream port for this downstream.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuration Examples for Extended Upstream Frequency Ranges

This section provides the following examples of sample configurations for the cable interface:

Example: Configuring North American (DOCSIS) Frequency Range

The following excerpt from a configuration file for the Cisco uBR7246VXR router shows a Cisco uBR-MC28U card and a Cisco uBR-MC16U card being configured for the default DOCSIS upstream frequency range of 5 MHz to 42 MHz. This frequency spectrum is allocated across two spectrum groups. Also, each downstream is configured for the DOCSIS Annex B mode.

Note The **cable freq-range north-american** command is not needed for this configuration, but using the command filters out the upstream frequencies above 42 MHz, which could be useful if noise is occurring in those frequencies.

```
...
cable freq-range north-american
cable spectrum-group 1 shared
cable spectrum-group 1 band 5000000 23500000
cable spectrum-group 2 shared
cable spectrum-group 2 band 23500000 42000000
...
!
interface Cable3/0
 description Cisco uBR-MC28U cable interface DS0
 ip address 10.2.4.1 255.255.255.0 secondary
 ip address 10.2.3.1 255.255.255.0
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 195000000
 cable downstream channel-id 0
 cable upstream 0 frequency 29008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 frequency 25808000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
```

```
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
 no cable upstream 1 shutdown
 cable upstream 2 frequency 9808000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 no cable upstream 2 shutdown
 cable upstream 3 frequency 19408000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 1
 no cable upstream 3 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
interface Cable3/1
 description Cisco uBR-MC28U cable interface DS1
 ip address 10.2.5.1 255.255.255.0 secondary
 ip address 10.2.4.1 255.255.255.0
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 789000000
 cable downstream channel-id 1
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 1
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 2
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 2
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 no cable upstream 3 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
interface Cable4/0
 description Cisco uBR-MC16U cable interface
 ip address 10.2.0.1 255.255.255.0 secondary
 ip address 10.2.0.1 255.255.255.0
 cable bundle 10 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 195000000
 cable downstream channel-id 2
 cable upstream 0 frequency 29008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 cable upstream 0 shutdown
 cable upstream 1 frequency 25808000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
```

```
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 frequency 9808000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 frequency 19408000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 35408000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000
 cable upstream 4 minislot-size 2
 cable upstream 4 modulation-profile 1
 cable upstream 4 shutdown
 cable upstream 5 frequency 16208000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 3200000
 cable upstream 5 minislot-size 2
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
...
```

Example: Configuring Japanese Frequency Range

The following excerpt from a configuration file for the Cisco uBR7246VXR router shows a Cisco uBR-MC28U card and two Cisco uBR-MC16U cards being configured for the Japanese extended upstream frequency range of 5 MHz to 55 MHz. This frequency spectrum is allocated across three spectrum groups. Also, each downstream is configured for the DOCSIS Annex B mode.

```
...
cable freq-range japanese
cable spectrum-group 1 shared
cable spectrum-group 1 band 5000000 23500000
cable spectrum-group 2 shared
cable spectrum-group 2 band 23500000 42000000
cable spectrum-group 3 shared
cable spectrum-group 3 band 42000000 55000000
...
!
interface Cable3/0
 description Cisco uBR-MC28U cable interface DS0
 ip address 10.2.4.1 255.255.255.0 secondary
 ip address 10.2.3.1 255.255.255.0
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 195000000
 cable downstream channel-id 0
 cable upstream 0 frequency 29008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 frequency 25808000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
```

```
 no cable upstream 1 shutdown
 cable upstream 2 frequency 44808000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 no cable upstream 2 shutdown
 cable upstream 3 frequency 19408000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 1
 no cable upstream 3 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
interface Cable3/1
 description Cisco uBR-MC28U cable interface DS1
 ip address 10.2.5.1 255.255.255.0 secondary
 ip address 10.2.4.1 255.255.255.0
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 789000000
 cable downstream channel-id 1
 cable upstream 0 frequency 45408000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 frequency 16208000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
 no cable upstream 1 shutdown
 cable upstream 2 frequency 6608000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 no cable upstream 2 shutdown
 cable upstream 3 frequency 41008000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 no cable upstream 3 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
interface Cable4/0
 description Cisco uBR-MC16U cable interface
 ip address 10.2.0.1 255.255.255.0 secondary
 ip address 10.2.0.1 255.255.255.0
 cable bundle 10 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 195000000
 cable downstream channel-id 2
 cable upstream 0 frequency 29008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 1
 cable upstream 0 shutdown
 cable upstream 1 frequency 25808000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 1
```

```
 cable upstream 1 shutdown
 cable upstream 2 frequency 9808000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 frequency 19408000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 35408000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000
 cable upstream 4 minislot-size 2
 cable upstream 4 modulation-profile 1
 cable upstream 4 shutdown
 cable upstream 5 frequency 16208000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 3200000
 cable upstream 5 minislot-size 2
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
interface Cable5/0
 description Cisco uBR-MC16U cable interface
 no ip address
 load-interval 30
 cable bundle 10
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 4
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 3
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 200000 200000
 cable upstream 0 minislot-size 32
 cable upstream 0 modulation-profile 41
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 1
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 42
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 3
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 42
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 3
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 42
 no cable upstream 3 shutdown
 cable upstream 4 spectrum-group 3
 cable upstream 4 ingress-noise-cancellation 200
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 42
```

```
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 3
 cable upstream 5 ingress-noise-cancellation 200
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 42
 no cable upstream 5 shutdown
 cable dhcp-giaddr policy
 cable helper-address 10.2.0.2
!
...
```

Example: Configuring European (EuroDOCSIS) Frequency Range

The following excerpt from a configuration file for the Cisco uBR10012 router shows a Cisco uBRMC5X20U card being configured for the EuroDOCSIS frequency range of 5 MHz to 65 MHz. This frequency spectrum is allocated across a number of spectrum groups. Also, each downstream is configured for the EuroDOCSIS Annex A mode.

```
...
card 5/0 5cable-mc520u-d
...
cable freq-range european
cable spectrum-group 1 shared
cable spectrum-group 1 band 5000000 42000000
cable spectrum-group 2 shared
cable spectrum-group 2 band 5000000 30000000
cable spectrum-group 3 shared
cable spectrum-group 3 band 30000000 42000000
cable spectrum-group 4 band 5000000 10000000
cable spectrum-group 5 band 10000000 15000000
cable spectrum-group 6 band 15000000 20000000
cable spectrum-group 7 band 20000000 25000000
cable spectrum-group 8 band 25000000 30000000
cable spectrum-group 9 band 30000000 35000000
cable spectrum-group 10 band 35000000 42000000
cable spectrum-group 12 band 42000000 50000000
cable spectrum-group 13 band 5000000 55000000
cable spectrum-group 14 band 55000000 65000000
!
interface Cable5/0/0
 no ip address
 cable enable-trap cmonoff-notification
 cable bundle 1 master
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream interleave-depth 64
 cable downstream frequency 471000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 6
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 21 22
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 7
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 121 122
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 8
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 800000
 cable upstream 2 minislot-size 8
 cable upstream 2 modulation-profile 123 124
 no cable upstream 2 shutdown
```

```
 cable upstream 3 spectrum-group 14
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 400000
 cable upstream 3 minislot-size 16
 cable upstream 3 modulation-profile 22 23
 no cable upstream 3 shutdown
!
interface Cable5/0/1
 no ip address
 load-interval 30
 cable bundle 1
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 471000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 10
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 122 123
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 2
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 124 125
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 3
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 400000
 cable upstream 2 minislot-size 16
 cable upstream 2 modulation-profile 126 127
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 1
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 200000
 cable upstream 3 minislot-size 32
 cable upstream 3 modulation-profile 125 128
 no cable upstream 3 shutdown
!
interface Cable5/0/2
 no ip address
 load-interval 30
 cable bundle 2
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream interleave-depth 16
 cable downstream frequency 453000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 21 22
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 2
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 122 129
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 3
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 800000
 cable upstream 2 minislot-size 8
 cable upstream 2 modulation-profile 123 126
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 1
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
```

```
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 22 23
 no cable upstream 3 shutdown
!
interface Cable5/0/3
 no ip address
 cable bundle 3
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream interleave-depth 16
 cable downstream frequency 471000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 6
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 21 22
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 6
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 121 122
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 7
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 800000
 cable upstream 2 minislot-size 8
 cable upstream 2 modulation-profile 123 124
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 7
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 400000
 cable upstream 3 minislot-size 16
 cable upstream 3 modulation-profile 22 23
 no cable upstream 3 shutdown
!
interface Cable5/0/4
 no ip address
 cable bundle 4
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 471000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 spectrum-group 10
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 22 24
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 10
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 2
 cable upstream 1 modulation-profile 122 129
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 15
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 minislot-size 2
 cable upstream 2 modulation-profile 125 124
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 15
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 minislot-size 2
 cable upstream 3 modulation-profile 22 23
 no cable upstream 3 shutdown
 no keepalive
!
```

Additional References

The following sections provide references related to the Extended Upstream Frequency Ranges.

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco Broadband Cable Command Reference Guide*, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Software Configuration Information	*Cisco uBR7100 Series Software Configuration Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/configuration/guide/scg7100.html *Cisco uBR7200 Series Software Configuration Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/configuration/guide/cr72scg.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html
Cable Features Configuration Guide	*Cisco CMTS Feature Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html
Cisco IOS Release 12.2 Command Reference	*Cisco IOS Release 12.2 Configuration Guides and Command References*, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

Standards and RFCs

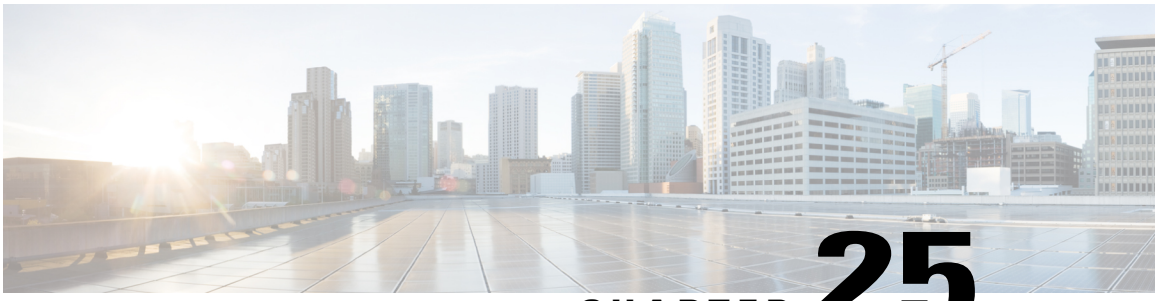
Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0

MIBs

MIBs	MIBs Link
• CISCO-CABLE-SPECTRUM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 25

Upstream Bonding Support for D-PON on the Cisco CMTS Routers

First Published: November 29, 2010

Cisco IOS Release 12.2(33)SCE provides support for the DOCSIS Passive Optical Network (D-PON). This architecture, also known as RF over glass (RFoG), helps the cable operators to effectively utilize the DOCSIS infrastructure and enter fiber-to-the-home market space.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Upstream Bonding Support for D-PON

The table below shows the hardware compatibility prerequisites for this feature.

Table 69: Upstream Bonding Support for D-PON Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 universal broadband router	Cisco IOS Release 12.2(33)SCE and later releases • PRE4 • PRE2 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V[47] • Cisco uBR-MC3GX60V[48]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCE and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC88V

47 The Cisco UBR-MC20X20V cable interface line card has three variants—Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

48 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

- DOCSIS 3.0 cable modems (CMs)
- DOCSIS 2.0 capable set-top boxes (STBs)
- You should configure the cable upstream ranging-init-technique 2 command to prevent the use of additional broadcast initial ranging opportunities for the non D-PON reference upstream channels.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Restrictions for Upstream Bonding Support for D-PON

- Multiple CMs cannot work at the same time. Each CM must get a separate time slot for upstream data transmission. Configuring D-PON ensures that the upstream scheduler allows only a single CM to transmit at a particular time.
- Configuring D-PON in a MAC domain enables D-PON for all MAC domains in the line card. Similarly, disabling D-PON on a MAC domain disables all the MAC domains in the line card.
- When D-PON is enabled in a MAC domain, you must manually shut down and enable the MAC domain using **shutdown** and **no shutdown** command.
- All frequencies in a MAC domain must have the same configuration for:

    - minislot size
    - channel-width
    - modulation profile

- Supports only ATDMA DOCSIS mode.
- The following features are not supported in MAC domains configured for D-PON:
    - Load balancing
    - Spectrum management
    - Upstream configuration (to change upstream configuration, you should shut down the MAC domain)
    - S-CDMA logical channels
    - Lower modulations profiles (D-PON uses only 16 QAM and 64 QAM modulation profiles)
    - Channel-width other than 3.2 MHz and 6.4 MHz
    - In-service Software Upgrade (ISSU)
    - Mixing of D-PON and HFC on the same MAC domain
    - Software licensing

Information About Upstream Bonding Support for D-PON

D-PON is a type of networking that allows the CMTS to transmit RF signals over the optical network. This technology enables the cable operators to use the RF technologies in a Hybrid Fiber-Coaxial (HFC) network.

The downstream data from the CMTS is combined with other RF signals at the hub and is sent to the transmitter. The signal from the transmitter is intended for multiple PONs. Each PON serves 32 homes from a single fiber.

The upstream data from the Optical Network Terminal (ONT) is combined at the splitter and sent to the hub, which is then routed to the optical receiver (RX). Upstream data from multiple optical receivers are combined and sent to the CMTS.

The upstream data to the CMTS contains signals from multiple PONs. Each upstream optical receiver is dedicated to a PON that can have multiple DOCSIS upstream sources (multiple modems and DSG terminals).

A PON can be configured in different ways, depending on the coaxial network. These configurations broadly fall under the following categories:

- Internal Control Configuration—In this configuration, the internal CM of the ONT controls the laser. Upstream signals go to the Ethernet interface of the CM allowing the ONT to control upstream timing. The device that uses this type of configuration is the Digital Audio Visual Council (DAVIC) set top terminal (STT).
- External Control Configuration—In this configuration, the presence of the RF at the ONT upstream input activates the laser. The device that uses this type of configuration is the DOCSIS Set-top Gateway (DSG) device.
- Dual Control Configuration—In this configuration, the home that contains an ONT with and internal CM and other DOCSIS upstream sources, like DSG devices. The RF presence detector or the internal CM control line detects the upstream signal and activates the upstream laser.

D-PON on Upstream Scheduling

In D-PON implementation, the native upstream scheduling software of the CMTS controls the timing of the upstream data transmission. Only one PON Receiver Domain (PRD) is allowed to transmit upstream data at any given point of time, irrespective of the upstream frequency allocation. The reason for this is that two lasers from the ONT of a PRD cannot work simultaneously as it leads to an Optical Beat Interference (OBI). Moreover, the use of a frequency modulation (FM) for and upstream signal transmission results in PHY errors when multiple ONTs within a PON transmits simultaneously.

Initial maintenance regions are scheduled on all upstream channels to prevent the DOCSIS 3.0 CMs in a D-PON environment from failing initial ranging on any upstream channel. When a ranging request is received within a MAC domain configured for D-PON, the CM receives an upstream channel override to the D-PON reference channel (US0).

In this implementation of D-PON, a DOCSIS device within a PRD is given a timeslot to transmit the upstream data, irrespective of the upstream frequency. Therefore, there is no benefit in having more than one upstream in a MAC domain without using the upstream channel bonding feature.

The D-PON feature supports the following service types:

- Best effort (BE) 3.0 using up to four frequencies concurrently
- BE 2.0 using only a single frequency
- Unsolicited grant service (UGS) using only a single frequency
- Real-time polling service (RTPS) using only a single frequency
- Non-real-time polling service (nRTPS) using only a single frequency

How to Configure Upstream Bonding Support for D-PON

This section describes how to enable D-PON for a MAC domain on the Cisco CMTS routers:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/port* | *slot/subslot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/0/1`	Enters interface configuration mode for the specified cable interface. The valid values are: • *slot*—5 to 8

	Command or Action	Purpose
		• *port*—0 to 4 (depending on the cable interface) • *subslot*—0 or 1 • *cable-interface-index* —0 to 14 (depending on the cable interface)
Step 4	**cable upstream dpon** **Example:** `Router(config-if)# cable upstream dpon`	Enables D-PON for a MAC domain.
Step 5	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to the privileged EXEC mode.

DOCSIS 3.0 Cable Modems Upstream Bonding Enters Partial Bonding

Sometimes, upstream bonding enters partial bonding while reverting to the original CLC after switchover. In the following example, the switchover is performed between CLC in slot 1 and 0. After reverting to CLC in slot 1, C1/0/3/UB turns to C1/0/3/p. The following output highlights the change:

```
Router# show cable modem
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2% Time source is NTP, 13:00:25.570
 UTC Thu Feb 18 2016

                                                                                    D
MAC Address    IP Address      I/F           MAC               Prim  RxPwr  Timing Num I
                                             State             Sid   (dBmv) Offset CPE P
4844.8789.e0fc 10.78.100.6     C1/0/0/UB     w-online          6     -0.50  1787   0   N
c8fb.2639.33d0 10.78.100.7     C1/0/1/UB     w-online          1     -1.00  1793   0   N
4844.8789.e10e 10.78.100.10    C1/0/2/UB     w-online          1     -0.50  1784   0   N
602a.d0a2.9b3e 10.78.100.11    C1/0/3/p   w-online          4     1.50   1789   0   N
0025.2ecf.f922 10.78.100.8     C1/0/4/UB     w-online          1     -1.00  1788   0   N
```

This partial bonding can be recovered using the **shutdown** and **no shutdown** commands on the related upstream port under the controller. The following is a sample configuration:

```
Router(config)# controller Upstream-Cable 1/0/3
Router(config-controller)# us-channel 0 shutdown
Router(config-controller)# no us-channel 0 shutdown
```

Verifying the Upstream Bonding Support for D-PON

To verify the upstream scheduler output for a MAC domain configured with D-PON, use the **show interface cable mac-scheduler** command.

Note The D-PON reference channel (US-1) MAP serves as a template for producing other MAPs within the MAC domain. Therefore, some of the statistics related to upstream scheduling is not relevant for other channels, except for the D-PON reference channel.

```
Router# show interface cable 7/0/2 mac-scheduler 1
     DOCSIS 1.1 MAC scheduler for Cable7/0/2/U1: rate 15360000
     wfq:None
     Req Slots 124, Req/Data Slots 13
     Init Mtn Slots 2243, Stn Mtn Slots 5
     Short Grant Slots 0, Long Grant Slots 0
     Adv Phy Short Grant Slots 1, Adv Phy Long Grant Slots 0
     Adv Phy UGS Grant Slots 0
     Awacs Slots 0
     Fragmentation count 0
     Fragmentation test disabled
     Avg upstream channel utilization : 0%
     Avg percent contention slots : 97%
     Avg percent initial ranging slots : 3%
     Avg percent minislots lost on late MAPs : 0%
     Sched Table Rsv-state: Grants 0, Reqpolls 0
     Sched Table Adm-State: Grants 0, Reqpolls 0, Util 0%
     UGS    : 0 SIDs, Reservation-level in bps 0
     UGS-AD : 0 SIDs, Reservation-level in bps 0
     RTPS   : 0 SIDs, Reservation-level in bps 0
     NRTPS  : 0 SIDs, Reservation-level in bps 0
     BE     : 0 SIDs, Reservation-level in bps 0
     MAP TSS: lch_state 13, init_retries 0
              late_initial_maps 0, late_ucd_maps 0
              mac-phy tss errors 0
! Only the D-PON reference channel will display the following
     Queue[Rng Polls] 0/128, 0 drops, flows 0 max 3
     Queue[CIR Grants] 0/256, 0 drops, flows 0 max 1
     Queue[BE(7) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(6) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(5) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(4) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(3) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(2) Grants] 0/64, 0 drops, flows 0 max 2
     Queue[BE(1) Grants] 0/64, 0 drops, flows 0 max 0
     Queue[BE(0) Grants] 0/64, 0 drops, flows 0 max 1
     BG pending grant list entries: 0
     BG delay list entries: 0
```

Additional References

The following sections provide references related to the Upstream Bonding Support for D-PON feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference

Related Topic	Document Title
Prisma D-PON	Cisco Prisma D-PON

Standards

Standards	Title
SCTE IPS SP 910	IPS SP 910 RFoG System http://www.ieee802.org/3/minutes/nov08/1108_SCTE_IPS_WG5_to_802_3.pdf

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Upstream Bonding Support for D-PON on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 70: Feature Information for Upstream Bonding Support for D-PON on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Upstream Bonding Support for D-PON	12.2(33)SCE	This feature was introduced for the Cisco uBR10012 and Cisco uBR7200 series Universal Broadband Routers. The following commands are new or modified: • **cable upstream dpon** • **show interface cable mac-scheduler**

CHAPTER 26

Upstream Channel Bonding

First Published: November 16, 2009

Last Updated: June 16, 2014

The Upstream Channel Bonding (USCB) feature helps cable operators offer higher upstream (US) bandwidth per cable modem (CM) user by combining multiple radio frequency (RF) channels to form a larger bonding group at the MAC layer.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Upstream Channel Bonding

- Enable downstream channel bonding before configuring the Upstream Channel Bonding feature on a Cisco cable modem termination system (CMTS) router.
- Ensure that the CM is registered in Multiple Receive Channel (MRC) mode before configuring upstream channel bonding on a Cisco CMTS router.
- Ensure that the CM is DOCSIS 3.0 certified.

The table below shows the hardware compatibility prerequisites for the Upstream Channel Bonding feature.

Table 71: Cable Hardware Compatibility Matrix for Upstream Channel Bonding

Cisco CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 router	Cisco IOS Release 12.2(33)SCC and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR10-MC5X20H • Cisco uBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[49]
Cisco uBR7246VXR router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V
Cisco uBR7225VXR router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

49 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

Restrictions for Upstream Channel Bonding

The following are the general restrictions for the Upstream Channel Bonding feature:

- Only the static bonding groups are supported in Cisco IOS Release 12.2(33)SCC and later.
- Only the upstream channels belonging to the same MAC domain can be added to an upstream bonding group.

Note Starting from Cisco IOS-XE 3.18.0S release, maximum of 16 upstream channels can be configured for each MAC Domain, which are divided into two groups:

- Group 1: upstream channel 0-7
- Group 2: upstream channel 8-15

The **upstream bonding-group** should include all the upstream channels either from Group 1 or Group 2 only.

- Committed information rate (CIR) oversubscription is not supported on USCB groups.

  Cisco CMTS allows oversubscription of the available bandwidth for individual upstream channels. However, oversubscription of bandwidth is not supported for USCB groups.

  An individual upstream may get oversubscribed due to static CIR service flows created for voice traffic. This may cause the DOCSIS 3.0 CMs with USCB to come online on single channel US bonding group (also known as default bonding group).

  This problem is mainly encountered in the voice deployments using static service flows. It is, therefore, recommended to choose from the following voice deployments such that the CIR is allocated (or released) when a voice call is attempted (or dropped):

  1. Dynamic Quality of Service (DQoS) Lite
  2. Packet Cable (PC) DQoS
  3. Packet Cable Multimedia (PCMM)

  These deployments avoid the individual upstream oversubscription and CMs come online on expected bonding groups.

Information About Upstream Channel Bonding

DOCSIS 3.0-based upstream channel bonding is a method for increasing upstream bandwidth up to a maximum of 120 Mbps raw throughput per CM user in a cable communications system that includes a Cisco CMTS router and multiple CMs. The upstream channel bonding method enables a CM to transmit data to a Cisco CMTS router on multiple upstream channels simultaneously.

Channel bonding is a method by which smaller bandwidth upstream channels are bonded together to create a larger upstream bonding group in the MAC domain. A MAC domain is a logical sub-component of a Cisco CMTS router and is responsible for implementing all DOCSIS functions on a set of downstream and upstream channels.

The Upstream Channel Bonding feature supports upstream traffic in Multiple Transmit Channel (MTC) mode for data and video services as these services require more bandwidth than voice-based services. Voice-based services either use the traditional single upstream channel or a single upstream channel bonding group configuration. Any traffic contract that exceeds 30 Mbps requires upstream channel bonding as the physical capacity of a single RF channel in DOCSIS cannot exceed 30 Mbps.

The Upstream Channel Bonding feature is supported on the Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCC and later. Upstream data from the subscriber comes through the upstream ports (US0-US19) that are automatically configured on the cable interface line card. The cable interface line card processes the data and sends it across the backplane to the WAN card and out to the Internet.

The table below lists the downstream and upstream frequencies supported on the various cable interface line cards.

Table 72: Downstream and Upstream Frequencies

Line Card	Downstream Frequency	Upstream Frequency
Cisco uBR10-MC5X20H	55-858 MHz	The upstream frequency range changes according the region and Annex A or Annex B configuration. • Annex A (EuroDOCSIS)—5 to 65 MHz • Annex B (DOCSIS, North American)—5 to 42 MHz • Annex B (J-DOCSIS)—5 to 55 MHz
Cisco uBR10-MC20X20V	55-999 MHz	
Cisco uBR-MC88V	69-999 MHz	
Cisco uBR-MC3GX60V	55-999 MHz[50]	The upstream frequency range for the Cisco uBR-MC3GX60V line card is from 5 to 85 MHz irrespective of the region and Annexure configuration.

50 This frequency range is subjected to the frequency restriction of the attached EQAM device.

Multiple Transmit Channel Mode

Multiple Transmit Channel mode is a CM capability that enables CMs to send upstream traffic on multiple upstream channels. You can enable the MTC mode on a cable interface line card in two ways:

- MTC mode on a per-CM basis—By default, the MTC mode is enabled with the required attribute. With this default configuration, the Cisco CMTS router enables the MTC mode on a per-CM basis depending on the CM configuration file. For more information about the default MTC mode configuration, see Default MTC Mode Configuration on a Cisco CMTS Router, on page 677.
- MTC mode for all CMs in a MAC domain—The MTC mode for all CMs in a MAC domain is disabled by default on an upstream bonding capable cable interface line card. You can enable MTC mode for all CMs in a MAC domain using the **cable mtc-mode** command in cable interface configuration mode.

Multiple Receive Channel Mode

MRC mode is a CM capability that enables CMs to receive downstream traffic on multiple downstream channels. The MRC mode is enabled by default on an upstream bonding capable cable interface line card. You can enable or disable the MRC mode in the MAC domain during or after the CM registration using the **cable mrc-mode** command.

Dynamic Range Window and Transmit Power Levels for Upstream Channel Bonding

The dynamic range window functionality is based on the CableLabs DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification and DOCSIS 3.0 Specification. This requires a DOCSIS 3.0 CM to have upstream transmit channel power level within a 12 dB range for all channels in its transmit channel set (TCS).

DOCSIS 1.x or 2.0 CMs operating with a single upstream channel, in non-MTC mode, have a higher maximum transmit power level than DOCSIS 3.0 CMs operating in the MTC mode with two or more upstream channels. That is, the maximum transmit power level per channel is reduced in the MTC mode.

When the upstream attenuation exceeds the maximum transmit power level, a DOCSIS 3.0 CM attempting to register in the MTC mode may fail to come online, or register in partial mode. The CM fails to register when the transmit power level of all upstream channels in its TCS exceeds the maximum transmit power level. If the CM has some upstream channels that are within the maximum transmit power level, the CM may come online in partial mode. However, the upstream channels that exceed the maximum transmit power level are marked as down and cannot be used for upstream traffic.

To verify the transmit power levels on a CM, use the show cable modem command with the verbose keyword. This command displays the following transmit power values for each assigned upstream channel:

- Reported Transmit Power—This is the reported transmit power level by the CM for each upstream channel.
- Minimum Transmit Power—This is the minimum transmit power level that the CM in the MTC mode could transmit at for the upstream channel.
- Peak Transmit Power—This is the maximum transmit power level that the CM in the MTC mode could transmit at for the upstream channel.

To support upstream channel bonding, the minimum transmit power must be less than or equal to the reported transmit power, and the reported transmit power must be less than or equal to the peak transmit power. The peak transmit power and minimum transmit power levels are derived from the CM TCS assignment and each individual upstream channel configuration.

If the minimum transmit power is higher than the reported transmit power, or the reported transmit power is higher than the peak transmit power, the CM may not come online or may register in partial mode.

You can troubleshoot this transmit power problem in the following two ways:

- Insert an additional amplifier to reduce the upstream attenuation so that the upstream transmit power falls within the allowed transmit power range (12 dB).
- Disable the MTC mode. To switch the CM from the MTC mode to non-MTC mode, disable the bonded-bit (bit-0) in type, length, value (TLV) 43.9.3 using the CM configuration file.

Extended Transmit Power

During the early deployment of DOCSIS 3.0 CMs, additional power is required from the CMs in order to compensate for the attenuation in the upstream path. CMs should transmit at extended power level than that defined in DOCSIS. This scenario is generally observed when USCB is enabled at the Cisco CMTS and the DOCSIS 3.0 CMs are operating in MTC mode.

Additional upstream power provides the operator with a power margin that helps overcome the upstream signal loss, reduces the cable plant operational cost, and enables rapid deployment of DOCSIS 3.0 CMs.

The Cisco CMTS supports the following features with which the CMs can transmit data at an extended power:

- Cisco Extended Transmit Power Feature
- DOCSIS Extended Transmit Power Feature

Cisco Extended Transmit Power Feature

The Cisco Extended Transmit Power feature, introduced in Cisco IOS Release 12.2(33)SCE3, supports DOCSIS 3.0 CMs operating in MTC mode to transmit at a higher power level than the power level specified in the *DOCSIS 3.0 Specification*. This feature is supported only with Cisco DPC3000 CMs.

The Cisco Extended Transmit Power feature enables cable operators to have better control on the cable modems that register in 4-channel or 2-channel MTC mode or in non-MTC mode to transmit at a higher power level than the DOCSIS-defined maximum power level. The cable operator can configure extended transmit power using the **cable tx-power-headroom** command in global configuration mode.

DOCSIS Extended Transmit Power Feature

The DOCSIS Extended Transmit Power feature, introduced in Cisco IOS Release 12.2(33)SCF2, supports extended upstream transmit power capability as defined in the DOCSIS3.0 Specification. This feature allows the CMs to transmit at a high extended power level to counter the attenuation in the US channel.

The table below lists the new TLVs supported by the DOCSIS Extended Transmit Power feature.

Table 73: TLVs for DOCSIS Extended Power Feature

TLV Name	Type	Length	Value
Extended Upstream Transmit Power Support	16	1	0—Extended Upstream Transmit Power Support Off 1—Extended Upstream Transmit Power Support On 2-255—Reserved
Extended Upstream Transmit Power CM Capability	5.40	1	0, 205-244 (units of one-quarter dB)

The Cisco CMTS sends TLV16 to inform the CM if the DOCSIS Extended Transmit Power feature is enabled. The CM in turn, sends TLV5.40 to the Cisco CMTS to communicate its extended power capability. After the negotiations are complete, the CM can transmit at an extended power.

DOCSIS Extended Transmit Power feature is enabled by default. Use the cable upstream ext-power command to enable or disable this feature. For more information on how to enable or disable DOCSIS Extended Power feature, see Configuring DOCSIS Extended Transmit Power Feature, on page 691.

Note DOCSIS Extended Transmit Power feature takes precedence, if both Cisco Extended Transmit Power feature and DOCSIS Extended Transmit Power feature are configured.

Reduced Transmit Channel Set

The Reduced Transmit Channel Set feature, introduced in Cisco IOS Release 12.2(33)SCE3, enables the Cisco CMTS router to reduce upstream channel set assignment based on the total power budget of the CM. For example, a reduction from four to two upstream channels gains 3 dB headroom. Further reduction from two channels to a single channel gains another 3 dB headroom, and the CM starts operating in non-MTC mode.

In order to take advantage of the reduced upstream channel set, the corresponding static bonding groups must be configured. For example, a MAC domain is configured with a bonding group having four channels. A CM with the reduced channel set of two is unable to match to the 4-channel bonding group, and can only be matched to a bonding group with two channels or less.

The Reduced Transmit Channel Set feature is helpful when a DOCSIS 3.0 CM is required to increase its total transmit power by 3 dB. For example, a DOCSIS 1.0 or 2.0 CM supports a maximum transmit power of 58 dBmV for Quadrature Phase Shift Keying (QPSK) modulation, while a DOCSIS 3.0 CM supports a maximum transmit power of 61 dBmV. In this case, the DOCSIS 3.0 CM operating in 4-channel MTC mode has a reduction in the maximum transmit power per upstream channel. This feature enables the Cisco CMTS router to support reduced input power level by 6 dB to prevent upstream path attenuation.

T4 Multiplier

T4 multiplier is the T4 timeout multiplier value of the default T4 timeout values as defined in for cable modems that are in the MTC mode. The default value is derived from the number of channels in the modem transmit channel set. You can change the default T4 multiplier value using the cable upstream ranging-poll command in cable interface configuration mode.

The T4 timeout multiplier values range is from 1 to 10. If the T4 multiplier value is equal to 1, the cable modem will T4 time out in 30 seconds (that is, 1 x 30 = 30). If you change the T4 multiplier to 4, then the new T4 timeout value will be 120 seconds (that is, 4 x 30 = 120).

Note If the T4 timeout multiplier is not configured from the range (1 - 10), then the CMTS uses the T4 timeout value of modem as T4 timeout value. For example, if the T4 timeout of the modem is 90 seconds, then the CMTS applies 3 as the T4 multiplier.

In the MTC mode, you can increase the T4 timeout value in order to reduce the router overhead associated with processing of ranging request (RNG-REQ) slots and ranging response messages. If an RNG-RSP message does not contain a T4 timeout multiplier value, then the CM uses the default T4 timeout value.

Fiber Node Configuration for Upstream Channel Bonding

The fiber node configuration on a Cisco CMTS router is used to define MAC domain downstream service groups (MD-DS-SGs) and MAC domain upstream service groups (MD-US-SGs) as defined in DOCSIS 3.0. Only the DOCSIS 3.0 certified modems use this information.

In hybrid fiber coaxial (HFC) networks, all CMs connected to the same coaxial segment of a fiber node reach the same set of downstream and upstream channels on one or more Cisco CMTS routers located at the headend.

A CM is physically connected to only one fiber node. The fiber node must include at least one primary-capable channel for the CM connected to the fiber node to be operational. The fiber node can include one or more primary-capable channels either from the cable interface line card, or from the primary-capable Shared Port Adaptor (SPA) downstream channels, or both.

Note When upgrading from Cisco IOS Releases 12.3(23)BC, 12.2(33)SCA, and 12.2(33)SCB to Cisco IOS Release 12.2(33)SCC and later, ensure that you add downstream and upstream connectors to the fiber node configuration. The fiber node configuration must be done in accordance with the physical plant topology. For details about the fiber node configuration, see the *Cable Fiber Node Best Practices for the Cisco uBR10012 Router* document at the following URL: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a00807f32fd.shtml

New TLVs for Upstream Channel Bonding

The table below lists the new CableLabs defined type, length, values (TLVs) for the Upstream Channel Bonding feature.

Table 74: New TLVs for Upstream Channel Bonding

TLV Name	Type	Length	Value
CM vendor ID	43.8	3	Per vendor definition
Cable modem attribute mask	43.9	n	Cable modem attribute mask subtype encodings

A Cisco CMTS can have multiple upstream channel bonding groups (USBG) configured. Each of these bonding groups can include upstream channels with different upstream frequencies. Some bonding groups can include channels with frequencies within the extended frequency range (see Table 72: Downstream and Upstream Frequencies, on page 668). An HFC network consists of several types of CMs, each supporting standard or extended upstream frequencies.

When you register a CM, the Cisco CMTS does not assign bonding groups based on the upstream frequency range supported by that CM. The assignment of the bonding groups is done to balance the CM count on each of the bonding groups. This may lead to assignment of a bonding group, in the extended frequency range, to a CM that lacks the extended frequency support. As a result, the CM will not be able to register. This scenario is generally observed in the Cisco uBR-MC3GX60V line card deployment (containing a mix of CMs), which supports frequency as high as 85MHz (see Table 72: Downstream and Upstream Frequencies, on page 668).

If the Cisco CMTS assigns a USBG with a channel within the extended frequency range to a CM limited to the standard frequency range, that CM may not be able to register on that upstream bonding group. Use the TLV 43.9.3 (CM US Required Attribute Mask) or TLV 43.9.4 (CM US Forbidden Attribute Mask) as a workaround. These TLVs enable the Cisco CMTS to assign CM to a USBG, which is in the upstream frequency range supported by that CM.

The default attributes (in hexadecimal) on a CM Attribute Mask (TLV 43.9) are “80 00 00 00", which means by default the mask is all zeroes with the bonding bit enabled. The first four bytes are pre-defined while the last four bytes are user defined. In order to enable Cisco CMTS to assign bonding groups based on the frequency range supported by CMs, complete these steps:

1. Configure a mask, using TLV 43.9.3 or TLV 43.9.4, by modifying the last four bytes. The mask should be configured such that a unique attribute is assigned to each of the bonding groups.

2 Apply this mask to the CM configuration file. CMs supporting extended frequency, can register with any USBGs, irrespective of the configured frequency range of the USBG. CMs supporting standard frequency, can only register with USBGs that are configured with standard frequency range.

Apply the mask you have configured above, to the CMs that support standard or extended frequency ranges. However, the ONLY CMs that need to employ the attribute mask are the ones with the standard frequency range, since they will not be able to register with the USBG configured with extended upstream frequency range. No attribute mask on the extended frequency supporting CMs means that these modems will be assigned any USBG.

The Cisco CMTS uses this mask, received in the CM configuration file during registration, to decide which USBG should be assigned to the CM.

Upstream Weighted Fair Queuing

The upstream weighted fair queuing (WFQ) is a quality of service (QoS) feature that enables the Cisco CMTS router to allocate optimum bandwidth to upstream service flows based on the WFQ parameter configurations. To enable upstream WFQ, you must configure either the class-based or activity-based WFQ on a cable interface.

The following WFQ parameter configurations are supported in Cisco IOS Release 12.2(33)SCD2 and later:

Class-Based Weighted Fair Queuing

In the class-based weighted fair queuing configuration, allocation of available bandwidth is dependent on the service flows that are active in a service class. A service class is a group of queuing attributes configured on the Cisco CMTS router. The class must have at least one active service flow. The class receives its portion of the available bandwidth based on the weight of the class. By default, each class (0 to 7) has a weight of "class + 1." For example, the class 0 has a weight of 1, and class 1 has a weight of 2.

Activity-Based Weighted Fair Queuing

In the activity-based weighted fair queuing configuration, allocation of available bandwidth is based on the service class and the total number of service flows that are active in a map for the service class. A service class with higher number of service flows receives the larger percentage of bandwidth.

Custom Weight for Service Flow Priorities

The weighted fair queuing functionality helps the Cisco CMTS router share the available bandwidth based on the weight of the service flow priorities specified for outstanding requests from an upstream service flow. Priority refers to the service flow priority specified in the CM configuration file, or the Cisco CMTS service class configuration. By default, the weight of a priority is equal to "priority+1." For example, priority 0 has a weight of 1, and priority 1 has a weight of 2. A higher priority provides more weight to the outstanding request. The custom weight can be specified for a total of eight priorities (0 to 7) in a service class.

The priority parameter refers to the priority of traffic in a service flow ranging from 0 (the lowest) to 7 (the highest). In the upstream traffic, all of the pending high priority service flows are scheduled for transmission before low priority service flows. You can configure the weight for priorities based on how much weight is appropriate per priority.

The table below lists the default weight for each service flow priority.

Table 75: Default Weight of Service Flow Priorities

Service Flow Priority	Default Weight
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Upstream Scheduler and Service Flows

A DOCSIS-qualified Cisco CMTS router can provide varied upstream scheduling modes for different packet streams or applications using upstream service flows. A service flow represents either an upstream or a downstream flow of data. A unique service flow ID (SFID) identifies each service flow. Each service flow can have its own quality of service (QoS) parameters, such as maximum throughput, minimum guaranteed throughput, and priority. In the case of upstream service flows, you can also specify a scheduling mode.

Scheduling is a process that enables the Cisco CMTS router to receive bandwidth requests and grant timeslots to CMs for the upstream traffic. The Cisco CMTS router periodically creates a grant map for each enabled upstream channel. The map grants individual timeslots to enable CMs to place packets on the upstream channels.

DOCSIS 3.0 describes a method by which a CM creates an upstream service flow. The following scheduling types enable the Cisco CMTS router to allocate bandwidth for upstream service flows:

- Unsolicited grant service (UGS)
- Solicited grant service

The unsolicited grant service is primarily used for voice. In the case of UGS, the CM does not have to explicitly request grants from the Cisco CMTS router whereas in the solicited grant service the CM has to explicitly request grants from the Cisco CMTS router. The solicited grant service is primarily used for best effort (BE) services.

Unlike DOCSIS 2.0, DOCSIS 3.0 allows multiple outstanding requests per service flow. For more information about the upstream scheduler, see the *Upstream Scheduler Mode for the Cisco CMTS Routers* feature guide at the following URL:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_upstm_sch_md_ps2209_TSD_Products_Configuration_Guide_Chapter.html

Distribution of Traffic across all Channels in a USBG

When upstream channel bonding (USCB) is enabled, the Distribution of Traffic across all Channels in a USBG feature can be used to balance the bandwidth utilization across upstream channels on one upstream bonding group.

This feature balances the utilization only if there is one upstream channel bonding group configured per MAC domain.

Restrictions:

- This feature is supported only on one upstream bonding group under a MAC domain. When multiple upstream bonding groups are configured under a MAC domain, the utilization is unfair.
- All the channels must be configured in one upstream bonding group under the same MAC domain.
- This feature is used only for UB-online cable modems.

Effective from Cisco IOS Release 12.2(33)SCH2, the USCB Balancing Scheduler may be enabled or disabled using the **cable upstream balance-scheduler** command in the interface (config-if) configuration mode.

DOCSIS 3.0 Load Balancing with USBG Smaller than Cable Modem Capabilities

When using USCB in a service group with USBGs containing fewer upstream channels than the total upstream channel set with DOCSIS 3.0 load balancing enabled, the CMTS can assign a Transmit Channel Set (TCS) to DOCSIS 3.0 cable modems for potential use which falls outside of the configured USBG. The CMTS will try to bind smaller UBGs and default single channel bonding groups into a bigger channel set in order to increase the cable modem services. For example, a DOCSIS 3.0 cable modem receiving the larger TCS can use these additional channels for dynamic service flow addition. The DOCSIS 3.0 Load Balancing feature can also move cable modems to upstream channels that are not explicitly configured with USBGs as a result of the larger TCS.

If you activate DOCSIS 3.0 Load Balancing while using upstream bonding, ensure that the upstream bonding group configuration is embedded and aligned by performing the following:

- Configure USBGs, which is matched to cable modem capabilities within the service group, such as a 4 channel USBG, 2 channel USBG, and 3 channel USBG as applicable.
- Ensure that configured USBGs are optimal for the upstream channel set based on modem capabilities within the service group. For example, if four upstream channels are available, channels 0+1 and 2+3 should each be an USBG to avoid dynamic TCS creating sub optimal bonding scenarios.
- Alternatively, you can choose to shut down any upstream channels that is not configured in USBGs which is not be used for bonding.

Cisco uBR10-MC5X20H Line Card Rate Limiting

The rate limiting functionality enables you control the aggregated rate and CPU consumption of upstream traffic for DOCSIS 3.0 bonded service flows on the Cisco uBR10-MC5X20H line card. In Cisco IOS Release 12.2(33)SCC, this functionality is supported only on the Cisco uBR10-MC5X20H line card. The rate limiting functionality is configured by default on the Cisco uBR10-MC5X20H line card. However, the default configuration can be modified using the **cable upstream rate-limit-ccf** command.

The rate limiting functionality uses the following two rate limiting methods:

- Aggregated rate limiting—This is based on Peripheral Component Interconnect (PCI) bus aggregated throughput. The throughput is per line card for all bonded service flows. You can modify the default throughput and burst rate configuration. The maximum allowed throughput is 115 Mbps.
- CPU-based rate limiting—This method controls the CPU consumed by Continuous Concatenation and Fragmentation (CCF) and ensures that the line card functions properly when traffic is overloaded with bonded service flows. The default configuration allocates 50 per cent of CPU to CCF. You can modify the default CPU threshold value and burst rate as required.

SID Tracking

The service ID (SID) tracking functionality enables you to track events related to upstream bandwidth requests and processing of grants. The SID tracker module can track events for a maximum of two service flows per MAC domain. The SID tracker module tracks up to 40,000 events per service flow on a cable interface line card.

You can enable SID tracking for the following types of events:

- DOCSIS 2.0 bandwidth request
- DOCSIS 3.0 bandwidth request
- Grant
- Pending grant (due to traffic congestion)
- Pending grant (due to shaping)

You can enable SID tracking using the **track keyword** along with the **debug cable interface sid** command. To verify SID tracking, use the **show interface cable upstream debug** command in privileged EXEC mode.

Service ID Clusters

A Cisco CMTS router can assign one or more service ID clusters to the upstream bonded service flows (upstream service flows assigned to an upstream bonding group) at the time of service flow creation. A SID cluster contains one SID per upstream in a bonding group. A CM uses one of the SIDs defined in the SID cluster for the upstream interface when the CM sends a bandwidth request. The CM chooses a SID or a SID cluster based on the SID cluster switching criteria.

For example, assume that a CM has ranged on upstream channels from 1 to 4. The Cisco CMTS router creates a bonded service flow and assigns a single SID cluster to each upstream channel. That is SID1 for UP1, SID2 for UP2, SID3 for UP3, and SID4 for UP4. Now, the CM can send a bandwidth request using any of the four upstream channels. That is, the CM can request bandwidth on any of the upstream interfaces in the SID cluster using the SID defined for the particular upstream. The Cisco CMTS router grants bandwidth to the CM using any combination of upstream channels.

How to Configure Upstream Channel Bonding

Note Before configuring the Upstream Channel Bonding feature, ensure that the fiber node is configured. The fiber node must be configured in accordance with the physical plant topology. For details about the fiber node configuration, see the *Cable Fiber Node Best Practices for the Cisco uBR10012 Router* document at the following URL: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a00807f32fd.shtm

The following tasks describe how to configure Upstream Channel Bonding on the Cisco uBR10012 router:

Enabling MTC Mode on a Cisco CMTS Router

To section explains how to enable the MTC mode on a Cisco CMTS router.

Default MTC Mode Configuration on a Cisco CMTS Router

By default, the MTC mode required attribute is configured on a cable interface line card. With this default configuration, the Cisco CMTS router enables the MTC mode on a per CM basis depending on the configuration file of each CM. When the CM configuration file has the bonded-bit (bit-0) enabled in TLV 43.9.3 (cable modem upstream required attribute mask), the Cisco CMTS router enables the CM to come online in the MTC mode. If the CM configuration file does not have the bonded-bit on, the CM comes online in non-MTC mode.

For more information on how to add the required attribute in the CM configuration file, see Example: Enabling MTC Mode for a Single CM Using the CM Configuration File, on page 693.

Enabling MTC Mode for All CMs

Note This MTC mode configuration supersedes the default MTC mode configuration (per CM basis) with the required attribute. To disable the MTC mode for all CMs in a MAC domain, use the **no** form of the **cable mtc-mode** command. If the MTC mode is enabled and the forbidden mask of the upstream bonding in TLV 43.9.4 is disabled, the CM does not support the Upstream Channel Bonding feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable mtc-mode** **Example:** `Router(config-if)# cable mtc-mode`	Enables MTC mode at the MAC interface for all CMs.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Creating a Bonding Group

An upstream bonding group is created by combining multiple upstream channels together on a cable interface line card.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream bonding-group** *id* **Example:** `Router(config-if)# cable upstream bonding-group 200`	Creates the bonding group on the specified cable interface.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

What to Do Next

After creating an upstream bonding group, you must add upstream channels to the bonding group.

Adding Upstream Channels to a Bonding Group

Restriction DOCSIS 3.0-certified CMs support only four upstream channels on an upstream bonding group. These CMs do not accept additional upstream channels that are added to a bonding group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream bonding-group** *id* **Example:** `Router(config-if)# cable upstream bonding-group 200`	Creates the bonding group on the specified interface.
Step 5	**upstream** *number* **Example:** `Router(config-upstream-bonding)# upstream 1`	Enters upstream bonding configuration submode and adds an upstream channel to the upstream bonding group. Starting from Cisco IOS-XE 3.18.0S release, maximum of 16 upstream channels can be configured for each MAC Domain, which are divided into two groups:

	Command or Action	Purpose
		• Group 1: upstream channel 0-7 • Group 2: upstream channel 8-15 The **upstream bonding-group** should include all the upstream channels either from Group 1 or Group 2 only.
Step 6	**end** **Example:** `Router(config-upstream-bonding)# end`	Exits upstream bonding configuration submode and returns to privileged EXEC mode.

Adding Upstream Channel Ports to a Fiber Node

You must add upstream channel ports to a fiber node in order to complete the basic upstream channel bonding configuration on a cable interface line card. The fiber node must contain all upstream and downstream channels reached by the CMs.

Restriction

- Configuration of a fiber node is valid only if all upstream channels inside the fiber node have different upstream frequencies.
- For any two upstream channels mapped to the connectors in the same fiber node where a spectrum group is assigned to one upstream channel, and a frequency is assigned to the other upstream channel, any overlap between any bands associated with the spectrum group of the upstream channel and the frequency of the upstream channel will result in an invalid fiber node configuration. That is a fixed frequency cannot overlap with another upstream channel's available spectrum group bands.

Note The fiber node configuration must be done in accordance with the physical plant topology. For details about the fiber node configuration, see the *Cable Fiber Node Best Practices for the Cisco uBR10012 Router* document at the following URL: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a00807f32fd.shtml

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable fiber-node** *fiber-node-id* **Example:** `Router(config)# cable fiber-node 2`	Enters fiber node configuration mode.
Step 4	**upstream cable** *slot*/*subslot* **connector** *grouplist* **Example:** `Router(config-fiber-node)# upstream cable 5/0 connector 2`	Specifies the upstream channel ports for a fiber node.
Step 5	**end** **Example:** `Router(config-fiber-node)# end`	Exits fiber node configuration mode and returns to privileged EXEC mode.

Configuring the Class-Based Weighted Fair Queuing

In the case of a class-based configuration, allocation of available bandwidth is dependent on the service flows that are active in a service class.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.

	Command or Action	Purpose
Step 4	**cable upstream qos wfq class** **Example:** `Router(config-if)# cable upstream qos wfq class`	Enables class-based weighted fair queuing.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring the Activity-Based Weighted Fair Queuing

In the activity-based configuration, allocation of available bandwidth is based on the service class and the total number of service flows that are active in a map for the service class.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream qos wfq activity** **Example:** `Router(config-if)# cable upstream qos wfq activity`	Enables activity-based weighted fair queuing.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring Custom Weights for Service Flow Priorities

The WFQ functionality helps the Cisco CMTS router share the available bandwidth based on the weight of the service flow priorities specified for outstanding requests from an upstream service flow.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream qos wfq weights** *priority0-priority7* **Example:** `Router(config-if)# cable upstream qos wfq weights 10 20 30 40 50 60 70 80.`	Enables custom weight configuration for all the service flow priorities in a service class. **Note** You must specify custom weight values for all the eight service flow priorities (0 to 7) when you modify the default weights of priorities. The valid range is from 1 to 255.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring the SID Cluster

This section explains how to configure and assign a SID cluster to an upstream bonded service flow.

Note Configure the **cable sid-cluster-group num-of-cluster 2** command to achieve desired upstream bonded speeds. Alternatively, use a large upstream Max Traffic burst value in the cable modem file (such as 30 kB). The Max Concat burst value in the cable modem file need not be changed because DOCSIS 3.0 uses continuous concatenations and fragmentation (CCF) and can therefore use the default value of 3044 in the Max Concat field.

Note If the **cable sid-cluster-group** command is not used, the router accepts the default SID cluster configuration. By default, only one SID cluster is configured. Similarly, if the **cable sid-cluster-switching** command is not used, the router accepts the default SID cluster switchover criterion. That is, only one request can be made using the SID cluster.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable sid-cluster-group [dynamic | req-multiplier** *value* **| num-of-cluster** *number*] **Example:** `Router(config-if)# cable sid-cluster-group dynamic` `Router(config-if)# cable sid-cluster-group req-multiplier 12` `Router(config-if)# cable sid-cluster-group num-of-cluster 2`	Creates a SID cluster group.
Step 5	**cable sid-cluster-switching [max-outstanding-byte** *value* **| max-request** *value* **| max-time** *seconds* **| max-total-byte** *value***]** **Example:** `Router(config-if)# cable sid-cluster-switching max-outstanding-byte 4444` `Router(config-if)# cable sid-cluster-switching max-request 222` `Router(config-if)# cable sid-cluster-switching max-time 444` `Router(config-if)# cable sid-cluster-switching max-total-byte 67890`	Specifies SID cluster switchover criteria.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Effective with Cisco IOS Release 12.2(33)SCH3, use the **show running-config all** command to verify the SID cluster configuration. Following is a sample output of the command:

```
Router# show running-config all
.
.
.
cable sid-cluster-group num-of-cluster 1
cable sid-cluster-group dynamic
cable sid-cluster-group req-multiplier 4
```

Configuring the Channel Timeout for a Cable Modem

The channel timeout configuration allows you to specify the maximum time that a CM can spend performing initial ranging on the upstream channels described in the Registration Response (REG-RSP) and REG-RSP-MP messages. The default channel timeout value (60 seconds) is automatically configured.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable init-channel-timeout** *value* **Example:** `Router(config-if)# cable init-channel-timeout 160`	Specifies the maximum time that a CM can spend performing initial ranging on the upstream channels.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring Cable Upstream Resiliency

The cable upstream resiliency module ensures that a CM remains operational if one or more non-primary upstream service flows of the CM enter temporary or persistent error states. This module enables a Cisco CMTS router to handle various events and maintain the transmit channel set of each CM.

In the event of the primary upstream service flow failure, the upstream resiliency module forces the CM to go offline.

Starting with Cisco IOS Release 12.2(33)SCG, for a Multiple Transmit Channel (MTC) modem, the (NRTPS), Real-time Polling Service (RTPS), (UGS), and (UGS-AD) upstream service flows on an impaired upstream channel is moved to another good upstream channel in the cable modem without resetting the cable modem.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream resiliency**{**channel-down-detect** *number* | **modem-offline-detect** *number* | **on-failure** {**disable-channel** | **extended-ranging** | **reset-modem**} | **sf-move** {**NRTPS** | **RTPS** | **UGS** | **UGS-AD**} } **Example:** `Router(config-if)# cable upstream resiliency channel-down-detect 30` `Router(config-if)# cable upstream resiliency modem-offline-detect 16` `Router(config-if)# cable upstream resiliency on-failure disable-channel` `Router(config-if)# cable upstream resiliency sf-move NRTPS` `Router(config-if)# cable upstream resiliency sf-move RTPS` `Router(config-if)# cable upstream resiliency sf-move UGS` `Router(config-if)# cable upstream resiliency sf-move UGS-AD`	Configures upstream resiliency for bonded upstream service flows.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring Rate Limiting on the Cisco uBR10-MC5X20H Line Card

The rate limiting functionality is configured by default on the Cisco uBR10-MC5X20H line card. However, the default configuration can be modified using the cable upstream rate-limit-ccf command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable upstream rate-limit-ccf** [**aggregated-burst** *value* | **aggregated-throughput** *value* | **cpu-burst** *value* | **cpu-threshold** *value*] **Example:** `Router(config)# cable upstream rate-limit-ccf aggregated-burst 25000` `Router(config)# cable upstream rate-limit-ccf aggregated-throughput 540000` `Router(config)# cable upstream rate-limit-ccf cpu-burst 30` `Router(config)# cable upstream rate-limit-ccf cpu-threshold 60`	Configures rate limiting parameters for upstream bonded service flows on a cable interface line card. • **aggregated-burst** *value*—(Optional) Specifies the burst rate for aggregated throughput-based rate limiting in bits. The valid range is from 0 to 250000000. The default value is 8000000. • **aggregated-throughput** *value*—(Optional) Specifies the throughput value for throughput-based rate limiting in bits per second (bps). The valid range is from 0 to 540000000. The default value is 115000000. • **cpu-burst** *value*—(Optional) Specifies the CPU burst for CCF in percentage. The valid range is from 0 to 100. The default value is 10. • **cpu-threshold** *value*—(Optional) Specifies the CPU threshold for CCF in percentage. The valid range is from 0 to 100. The default value is 50.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Upstream Related Events for CM Status Reports

You can enable upstream related CM status events only on a cable interface line card. You can enable the following upstream related CM status events per interface using the cable cm-status enable command:

- T4 time-out
- T3 re-tries exceeded
- Successful ranging after T3 re-tries exceeded

For details on how to enable upstream and downstream related CM status events, see the Wideband Modem Resiliency feature guide at the following URL:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_wm_resiliency.html

Modifying the Bonding Group Attributes

Bonding group attributes are automatically configured for each upstream bonding group. You can modify them using the **attributes** command in upstream bonding configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream bonding-group** *id* **Example:** `Router(config-if)# cable upstream bonding-group 200`	Creates the bonding group on the specified cable interface and enters the upstream bonding configuration mode.

	Command or Action	Purpose
Step 5	**attributes** *value* **Example:** `Router(config-upstream-bonding)# attributes eeeeeeee`	Modifies the attribute value for the specified bonding group.
Step 6	**end** **Example:** `Router(config-upstream-bonding)# end`	Exits upstream bonding configuration mode and returns to privileged EXEC mode.

Modifying the Ranging Poll Interval on Upstream Channels

You can change the default ranging poll interval (20 seconds) on upstream channels using the cable upstream ranging-poll command in cable interface configuration mode. You can also specify the T4 timeout multiplier value using this command.

For information on T4 Multiplier, see T4 Multiplier, on page 671 .

Note We recommend that you do not modify the default ranging poll interval unless required. With the default configuration, a DOCSIS 2.0 CM in non-MTC mode performs ranging on one upstream channel every 20 seconds.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream ranging-poll** [**interval** *value* | **t4-multiplier** *timeout_value*]	Specifies the ranging poll interval for upstream channels.

	Command or Action	Purpose
	Example: `Router(config-if)# cable upstream ranging-poll interval 24000 t4-multiplier 4`	**Note** If **t4-multiplier** *timeout_value* is not configured, then the CMTS uses the the T4 timeout of the modem. For example, if the T4 timeout of the modem is 90 seconds, then the CMTS will apply 3 as T4 multiplier for the modem.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring the Reduced Channel Set Assignment

You need to configure the transmit power offset budget to enable the Cisco CMTS router to reduce upstream channel set assignment based on the total power budget of the CM.

Note The threshold value specified for the power budget offset (max-channel-power-offset) must be less than the power threshold value (power-adjust continue) that determines the value of the Ranging Status field in the Ranging Response (RNG-RSP) messages that the Cisco CMTS router sends to the CM. You can specify the power threshold value using the **cable upstream power-adjust** command.

Before You Begin

- Configure extended transmit power using the **cable tx-power-headroom** command in global configuration mode.
- Ensure that corresponding static bonding groups are configured.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*}	Specifies the cable interface line card on a Cisco CMTS router.

	Command or Action	Purpose
	Example: `Router(config)# interface cable 7/1/0`	
Step 4	**cable upstream max-channel-power-offset** *dB-value* **Example:** `Router(config-if)# cable upstream max-channel-power-offset 2`	Specifies the power offset value for upstream channels.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits cable interface configuration mode and returns to privileged EXEC mode.

Configuring DOCSIS Extended Transmit Power Feature

The DOCSIS Extended Transmit Power feature is enabled by default on the Cisco CMTS. However, the default configuration can be modified using the cable upstream ext-power command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot/subslot/port* | *slot/subslot/cable-interface-index* | *slot/port* | *slot/cable-interface-index*} **Example:** `Router(config)# interface cable 7/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable upstream ext-power** **Example:** `Router(config-if)# cable upstream ext-power`	Enables the DOCSIS Extended Transmit Power feature on the Cisco CMTS. Using the **no** form of this command disables the DOCSIS Extended Transmit Power feature.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following debug commands help you troubleshoot an improper upstream channel bonding configuration and its related features:

- **debug cable cm-status—**Provide debugging information about CM status messages on the Cisco CMTS routers.
- **debug cable mdd—**Provides debugging information about MAC domain descriptor (MDD).
- **debug cable md-sg—**Provides information about service group debugging messages.
- **debug cable ubg—**Provides debugging information about upstream bonding groups.

Configuration Example for Upstream Channel Bonding

The following example shows how to configure the basic upstream channel bonding on the Cisco uBR-MC3GX60V line card interface 8/1/14 on the Cisco uBR10012 router:

```
interface Cable 8/1/14
 downstream Modular-Cable 8/1/0 rf-channel 0
 downstream Modular-Cable 8/1/1 rf-channel 8
 downstream Modular-Cable 8/1/2 rf-channel 16
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 81
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 15000000
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 docsis-mode tdma
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 attribute-mask 20000000
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 25000000
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 docsis-mode tdma
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 attribute-mask 20000000
```

```
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 30000000
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 docsis-mode tdma
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 35000000
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 docsis-mode tdma
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
end
cable fiber-node 1
  downstream Modular-Cable 8/1/0 rf-channel 0-7
 upstream Cable 8/1 connector 0
!
cable fiber-node 13
  downstream Modular-Cable 8/1/1 rf-channel 8-15
 upstream Cable 8/1 connector 0
!
cable fiber-node 23
  downstream Modular-Cable 8/1/2 rf-channel 16-23
 upstream Cable 8/1 connector 0
```

Note Bonded channels are typically from the same connector; however, channels from different connectors in the same MAC domain can also be bonded together. A single MAC domain can support multiple channel bonding groups.

Note Only two channel frequency stacking is supported for Cisco uBR-MC5x20H and Cisco uBR-MC20x20 cable interface line cards.

Example: Enabling MTC Mode for a Single CM Using the CM Configuration File

The following example shows how to enable the MTC required attribute using the CM configuration file:

```
03 (Net Access Control) = 1
Unknown Type 005 = 01 01 01
18 (Maximum Number of CPE) = 4
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S10 (Min Reserved Traffic Rate)= 500000
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S10 (Min Reserved Traffic Rate) = 1000000
29 (Privacy Enable) = 0
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S009 (Unknown sub-type) = 03 04 80 00 00 00
```

Verifying the Upstream Channel Bonding Configuration

Use the following **show** commands to verify the upstream channel bonding configuration:

- **show cable mac-domain upstream-service-group**
- **show cable fiber-node**
- show interface cable upstream
- **show interface cable service-flow**
- **show cable modem**

To verify the runtime statistics of the upstream service group on a cable interface line card, use the **show cable mac-domain upstream-service-group** command as shown in the following example:

```
Router# show cable mac-domain cable 8/1/14 upstream-service-group
Cable MD 8/1/14
  US-SG-ID  : 1         US-Chan : U0,1,2,3
  Primary-DS: 8/1/0:0   US-SG-ID: 1
    MDD US-List   : U0,1,2,3
    MDD Ambiguity : U0,1,2,3
  Primary-DS: 8/1/1:8   US-SG-ID: 1
    MDD US-List   : U0,1,2,3
    MDD Ambiguity : U0,1,2,3
  Primary-DS: 8/1/2:16  US-SG-ID: 1
    MDD US-List   : U0,1,2,3
    MDD Ambiguity : U0,1,2,3
```

To verify the configuration of a fiber node, use the **show cable fiber-node** command as shown in the following example:

```
Router# show cable fiber-node
Fiber-Node 1
  Channels    :   downstream Modular-Cable    8/1/0:   0-7
  Channel IDs :   169, 170, 171, 172, 173, 174, 175, 176
  upstream Cable 8/1:  0
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
 ----------------------------------------------------------------
Fiber-Node 2
  Channels    :   downstream Modular-Cable    1/1/0:   0-1
  Channel IDs :   193, 194
  upstream Cable 5/0:  0
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
 ----------------------------------------------------------------
Fiber-Node 13
  Channels    :   downstream Modular-Cable    8/1/1:   8-15
  Channel IDs :   177, 178, 179, 180, 181, 182, 183, 184
  upstream Cable 8/1:  0
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
 ----------------------------------------------------------------
Fiber-Node 23
  Channels    :   downstream Modular-Cable    8/1/2:   16-23
  Channel IDs :   185, 186, 187, 188, 189, 190, 191, 192
  upstream Cable 8/1:  0
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
```

To verify the bonding groups configured on a cable interface line card, use the **show interface cable upstream** command as shown in the following example:

```
Router# show interface cable 8/1/14 upstream bonding-group
```

```
Cable8/1/14: Upstream Bonding Group 81
     12 packets input, 4614 octets input
     Segments: 12 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 10240000 bits/sec
     Total Service Flows On This Bonding Group: 1
Cable8/1/14: Upstream Bonding Group 65536
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 2560000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable8/1/14: Upstream Bonding Group 65537
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 2560000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable8/1/14: Upstream Bonding Group 65538
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 2560000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable8/1/14: Upstream Bonding Group 65539
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 2560000 bits/sec
     Total Service Flows On This Bonding Group: 0
```

To verify upstream bonding information on a cable interface line card, use the **show interface cable service-flow** command as shown in the following example:

```
Router# show interface cable 8/1/14 service-flow 19 verbose

Sfid                                  : 19
Mac Address                           : 001e.6bfb.3332
Type                                  : Primary
Direction                             : Upstream
Current State                         : Active
Current QoS Indexes [Prov, Adm, Act]  : [4, 4, 4]
Active Time                           : 1h25m
Required Attributes                   : 0x00000000
Forbidden Attributes                  : 0x00000000
Aggregate Attributes                  : 0x00000000
Sid                                   : 6
Traffic Priority                      : 0
Maximum Sustained rate                : 50000000 bits/sec
Maximum Burst                         : 3044 bytes
Minimum Reserved Rate                 : 0 bits/sec
Minimum Packet Size                   : 0 bytes
Admitted QoS Timeout                  : 200 seconds
Active QoS Timeout                    : 0 seconds
Packets                               : 0
Bytes                                 : 0
Rate Limit Delayed Grants             : 0
Rate Limit Dropped Grants             : 0
Current Throughput                    : 0 bits/sec, 0 packets/sec
Application Priority                  : 0
US Bonded                             : YES
Upstream Bonding Group                : UBG-65535
Transmit Channel Set                  : 0xF
Sid Cluster                           : SC-0, Sid [ 6 6 6 6 ]
Sid Cluster                           : SC-1, Sid [ 9 9 9 9 ]
Segments Valid                        : 0
Segments Discarded                    : 0
```

```
Segments Lost                           : 0
SID Cluster Switching Information
Total Bytes Requested                   : 0
Total Time                              : 20
Outstanding Bytes                       : 25600
Max Requests                            : 8
Classifiers: NONE
```

To verify the transmit power levels on a CM, use the **show cable modem** command as shown in the following example:

```
Router# show cable modem 0014.f831.d596 verbose
MAC Address                         : 001e.6bfa.f02e
IP Address                          : 30.10.0.6
IPv6 Address                        : ---
Dual IP                             : N
Prim Sid                            : 5
Host Interface                      : C5/1/0/UB
MD-DS-SG / MD-US-SG                 : 1 / 1
MD-CM-SG                            : 0xF0101
Primary Wideband Channel ID         : 48
Primary Downstream                  : Mo3/0/0:0 (RfId : 120)
Wideband Capable                    : Y
RCP Index                           : 3
RCP ID                              : 00 10 00 00 04
Multi-Transmit Channel Mode         : Y
Upstream Channel                    : US1        US2        US3        US4
Ranging Status                      : sta        sta        sta        sta
Upstream Power (dBmV)               : 0.00       0.00       0.00       0.00
Upstream SNR (dB)                   : 36.12      36.12      36.12      33.1
Received Power (dBmV)               : 0.00       1.00       0.00       -0.75
Reported Transmit Power (dBmV)      : 45.00      45.00      45.00      54.75
Peak Transmit Power (dBmV)          : 51.00      51.00      56.00      56.00
Minimum Transmit Power (dBmV)       : 24.00      24.00      21.00      18.00
Timing Offset              (97.6 ns): 2312       2281       2282       2282
Initial Timing Offset               : 2314       2058       2058       2058
Rng Timing Adj Moving Avg(0.381 ns): 7          4          0          -94
Rng Timing Adj Lt Moving Avg        : 63         30         11         -144
Rng Timing Adj Minimum              : -512       -256       -256       -512
Rng Timing Adj Maximum              : 256        57088      57344      57344
Pre-EQ Good                         : 0          0          0          0
Pre-EQ Scaled                       : 0          0          0          0
Pre-EQ Impulse                      : 0          0          0          0
Pre-EQ Direct Loads                 : 0          0          0          0
Good Codewords rx                   : 5012       4996       4992       4990
Corrected Codewords rx              : 0          0          0          0
Uncorrectable Codewords rx          : 0          0          0          0
Phy Operating Mode                  : atdma*     atdma*     tdma*      tdma*
sysDescr                            :
Downstream Power                    : 0.00 dBmV (SNR = ----- dB)
MAC Version                         : DOC3.0
QoS Provisioned Mode                : DOC1.1
Enable DOCSIS2.0 Mode               : Y
Modem Status                        : {Modem= w-online, Security=disabled}
Capabilities                        : {Frag=N, Concat=N, PHS=Y}
Security Capabilities               : {Priv=, EAE=Y, Key_len=}
L2VPN Capabilities                  : {L2VPN=N, eSAFE=N}
Sid/Said Limit                      : {Max US Sids=8, Max DS Saids=24}
Optional Filtering Support          : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support          : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE IPs                   : 0(Max CPE IPs = 16)
CFG Max-CPE                         : 4
Flaps                               : 0()
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 0 aborts, 0 exhausted
Total US Flows                      : 2(2 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 6 packets, 1557 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 0 packets, 0 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
LB group ID assigned (index)        : N/A (N/A)
```

```
LB group ID in config file (index) : N/A (N/A)
LB policy ID                       : 0
LB policy ID in config file        : 0
LB priority                        : 0
Tag                                :
Required DS Attribute Mask         : 0x0
Forbidden DS Attribute Mask        : 0x0
Required US Attribute Mask         : 0x0
Forbidden US Attribute Mask        : 0x0
Service Type ID                    :
Service Type ID in config file     :
Active Classifiers                 : 0 (Max = NO LIMIT)
CM Upstream Filter Group           : 0
CM Downstream Filter Group         : 0
CPE Upstream Filter Group          : 0
CPE Downstream Filter Group        : 0
DSA/DSX messages                   : permit all
Voice Enabled                      : NO
DS Change Times                    : 0
Boolean Services                   : 2
Number of Multicast DSIDs Support  : 24
MDF Capability Mode                : 2
IGMP/MLD Version                   : IGMPv3
FCType10 Forwarding Support        : Y
Features Bitmask                   : 0x0
Total Time Online                  : 1d16h
CM Initialization Reason           : NO_PRIM_SF_USCHAN
CFG Max IPv6 CPE Prefix             : 16 (-1 used)
```

Verifying Weighted Fair Queuing for Upstream Service Flows

To verify WFQ parameters configured for upstream service flows on a cable interface line card, use the **show interface cable mac-scheduler** command as shown in the following example:

```
Router# show interface cable 5/0/2 mac-scheduler 0
DOCSIS 1.1 MAC scheduler for Cable5/0/2/U0: rate 10240000
wfq:Class,  weights: 1  2  3  4  5  6  7  8
Queue[Rng Polls] 0/128, 0 drops, flows 0 max 0
Queue[CIR Grants] 0/256, 0 drops, flows 0 max 0
Queue[BE(7) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(6) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(5) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(4) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(3) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(2) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(1) Grants] 0/32, 0 drops, flows 0 max 0
Queue[BE(0) Grants] 0/32, 0 drops, flows 0 max 0
Queue[LLQ Grants] 0/64, 0 drops, flows 0 max 0
BG pending grant list entries: 0
BG delay list entries: 0
Req Slots 265389868, Req/Data Slots 4
Init Mtn Slots 3798558, Stn Mtn Slots 0
Short Grant Slots 0, Long Grant Slots 0
Adv Phy Short Grant Slots 0, Adv Phy Long Grant Slots 0
Adv Phy UGS Grant Slots 0
Awacs Slots 0
Fragmentation count 0
Fragmentation test disabled
Avg upstream channel utilization : 0%
Avg percent contention slots : 97%
Avg percent initial ranging slots : 3%
Avg percent minislots lost on late MAPs : 0%
Sched Table Rsv-state: Grants 0, Reqpolls 0
Sched Table Adm-State: Grants 0, Reqpolls 0, Util 0%
UGS    : 0 SIDs, Reservation-level in bps 0
UGS-AD : 0 SIDs, Reservation-level in bps 0
RTPS   : 0 SIDs, Reservation-level in bps 0
NRTPS  : 0 SIDs, Reservation-level in bps 0
BE     : 0 SIDs, Reservation-level in bps 0
```

```
MAP TSS: lch_state 11, init_retries 0
late_initial_maps 0, late_ucd_maps 0
mac-phy tss errors 0
r4k ticks in 1ms 800000
Total scheduling events 0
No search was needed 0
Previous entry free 0
Next entry free 0
Could not schedule 0
Recovery failed 0
Curr time 251 entry 251
```

Verifying Rate Limiting for Upstream Bonded Service Flows

To verify the rate limiting criteria configured on the Cisco uBR10-MC5X20H line card for upstream bonded service flows, use the **show cable rate-limit-ccf** command as shown in the following example:

```
Router# show cable rate-limit-ccf
rate_limiting config: aggr_throughput: 215000000 aggr_burst: 240000
cpu_threshold: 50 cpu_burst: 10
5X20H rate limit: cpu-throttle 0 ccf-bw-drop 0 others 0
5X20H rate limit ccf info count: 0
```

Note The **show cable rate-limit-ccf** command is applicable only to the Cisco uBR-MC5X20 cable interface line card.

Verifying Extended Power Transmission

To verify that a CM is transmitting at a higher power level, use the show cable modem command as shown in the following example:

```
Router# show cable modem 0022.2d56.d42d verbose
.
.
.
Multi-Transmit Channel Mode : Y
Upstream Channel : US1 US2 US3 US4
Ranging Status : sta sta sta sta
Upstream SNR (dB) :  36.12 36.12 36.12 36.12
Received Power (dBmV) : 1.00 !2.00 !2.00 !2.50
Reported Transmit Power (dBmV): 54.00 54.00 54.00 54.00
Peak Transmit Power (dBmV) : 51.00 51.00 51.00 51.00
Minimum Transmit Power (dBmV): 21.00 21.00 21.00 21.00
Timing Offset 97.6 ns) : 2311 2311 2310 2311
!Compare the Reported Transmit Power and Peak Transmit Power values to verify that the cable
 modem is transmitting at a higher power level.
.
```

To list all the CMs that are transmitting at higher power level, use the show cable modem extended-power command as shown in the following example:

```
Router# show cable modem extended-power
MAC Address    IP Address      I/F           MAC           Prim  Report  ECN
                                             State         Sid   Power
001e.6bfb.3382 5.50.0.3        C7/0/0/UB     w-online      3     57.00   Y
0022.cea5.0214 5.50.1.102      C7/0/0/UB     w-online      5     54.00   Y
001e.6bfb.1378 5.50.6.83       C7/0/0/UB     w-online      6     54.00   Y
```

Additional References

The following sections provide references related to the Upstream Channel Bonding feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
DOCSIS 3.0 Downstream Channel Bonding	*Cisco Cable Wideband Solution Design and Implementation Guide* http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_1.0/wb_solu.html
Cisco uBR10-MC5X20S/U/H Cable Interface Line Card	*Cisco uBR10-MC5X20S/U/H Cable Interface Line Card Hardware Installation Guide* http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/installation/guide/ubrmc520.html
Dynamic Bandwidth Sharing	*Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_dyn_bw_sharing_ps2209_TSD_Products_Configuration_Guide_Chapter.html
Upstream Scheduler Mode	*Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_upstm_sch_md_ps2209_TSD_Products_Configuration_Guide_Chapter.html

Standards and RFCs

Standard	Title
CM-SP-MULPIv3.0-I10-090529	Data-Over-Cable Service Interface Specifications DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification
CM-SP-PHYv3.0-I08-090121	Data Over Cable Service Interface Specifications DOCSIS 3.0 Physical Layer Specification

MIBs

MIB	MIBs Link
• DOCS-IF3-MIB • DOCS-SUBMGT3-MIB • CLAB-TOPO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Upstream Channel Bonding

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 76: Feature Information for Upstream Channel Bonding

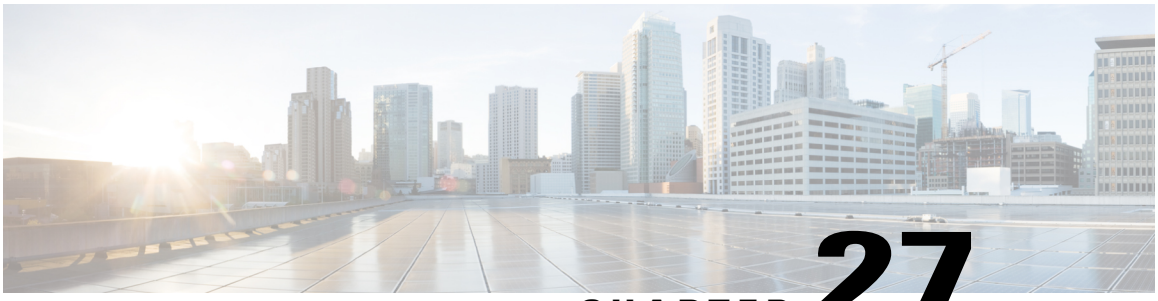
Feature Name	Releases	Feature Information
Upstream Channel Bonding	12.2(33)SCC	

Feature Name	Releases	Feature Information
		The Upstream Channel Bonding feature helps cable operators offer higher upstream bandwidth per CM user by combining multiple physical RF channels to form a larger bonding group at the MAC layer. The following sections provide information about this feature: • Information About Upstream Channel Bonding, on page 667 • How to Configure Upstream Channel Bonding , on page 677 • Configuration Example for Upstream Channel Bonding , on page 692 The following commands were introduced or modified: • **cable mtc-mode** • **cable mrc-mode** • **cable upstream bonding-group** • **cable upstream resiliency** • **cable upstream ranging-poll** • **clear cable modem cm-status** • **debug cable cm-ctrl** • **debug cable cm-status** • **debug cable mdd** • **debug cable md-sg** • **debug cable ubg** • **show cable fiber-node** • **show cable flap-list** • **show cable mac-domain upstream-service-group**

Feature Name	Releases	Feature Information
		• **show cable modem cnr** • **show cable signal-quality** • **show interface cable service-flow** • **show interface cable upstream** • **upstream** • **upstream cable connector**
Cisco uBR10-MC5X20H Line Card Specific Rate Limiting	12.2(33)SCC	The following commands were introduced: • **cable upstream rate-limit-ccf** • **show cable rate-limit-ccf**
SID Tracking	12.2(33)SCC	The following commands were introduced or modified: • **debug cable interface sid** • **show interface cable upstream debug**
Upstream Channel Bonding	12.2(33)SCD	Added support for Cisco uBR7246VXR and Cisco uBR7225VXR routers.
Upstream Weighted Fair Queuing	12.2(33)SCD2	Added support for class-based and activity-based weighted fair queuing configuration for upstream service flows. The following commands were introduced or modified: • **cable upstream qos wfq** • **show interface cable mac-scheduler**

Feature Name	Releases	Feature Information
Upstream Channel Bonding	12.2(33)SCE	The following commands were modified to support the Cisco uBR-MC3GX60V cable interface line card: • **interface cable** • **show interface cable** • **show running-config interface cable**
Extended Transmit Power and Reduced Transmit Channel Set	12.2(33)SCE3	The Extended Transmit Power feature enables cable operators to have better control on the CMs that register in 4-channel or 2-channel MTC mode or in non-MTC mode to transmit at a higher power level than the DOCSIS-defined maximum power level. The following commands were introduced or modified: • **cable tx-power-headroom** • **cable upstream max-channel-power-offset**
DOCSIS Extended Transmit Power	12.2(33)SCF2	This feature introduces the extended transmit power capability on the Cisco CMTS as per the DOCSIS specification. The DOCSIS 3.0 CMs can now transmit at a higher power level to overcome the signal loss because of the attenuation in the US path. The following commands were introduced or modified: • **cable upstream ext-power** • **show cable modem extended-power**

Feature Name	Releases	Feature Information
Upstream Channel Resiliency for RTPS Service Flows	12.2(33)SCG	This feature enables movement of the upstream service flows on an impaired upstream channel to another good upstream channel in the transmit channel set of the cable modem without resetting the cable modem. The following command was introduced: • **cable upstream resiliency sf-move**
Data-burst Resiliency Polling Interval	Cisco IOS-XE Release 3.18.0S	This feature enables to set data-stream resiliency polling interval of the upstream service flows. The following command was introduced: • **cable upstream resiliency data-burst polling-interval**



CHAPTER 27

Upstream Scheduler Mode for the Cisco CMTS Routers

First Published: December 18, 2008

Last Updated: June 20, 2011

Note Cisco IOS Release 12.2(33)SCA integrates support for the Upstream Scheduler Mode feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure optional upstream (US) scheduler modes.

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Upstream Scheduler Mode for the Cisco CMTS Routers

The table below shows the hardware compatibility prerequisites for this feature.

Table 77: Upstream Scheduler Mode for the Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • CiscoUBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[51]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[52]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

51 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

52 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Upstream Scheduler Mode for the Cisco CMTS Routers

- To ensure proper operation, Call Admission Control (CAC) must be enabled. When the 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.
- UGS with Activity Detection (UGS-AD) is not supported by the LLQ scheduler mode but remains supported by the default DOCSIS scheduler mode.
- Upstream bandwidth request rate limiting feature is supported only on the Cisco UBR-MC20X20V, Cisco uBR-MC3GX60V, Cisco uBR-MC88V, and Cisco uBR-MC5X20H cable interface line cards.

Information About Upstream Scheduler Mode for the Cisco CMTS Routers

With UGS, a service flow is created that enables a cable modem to transmit fixed-size bursts of data at a guaranteed rate and with a guaranteed level of jitter by providing periodic transmission opportunities to the cable modem for fixed-sized frames. This kind of service flow is particularly suitable for VoIP applications.

With rtPS, a service flow is created that provides a periodic opportunity for a cable modem to request permission to transmit data by polling a single cable modem for a bandwidth request, rather than all the cable modems. This satisfies applications that have a requirement for real-time data transmission, and enables the cable modem to transmit data bursts of varying length. This kind of service flow is particularly suitable for MPEG VoIP.

Starting with Cisco IOS Release 12.2(33)SCG, rtPS requests, by default, are internally treated as priority 7—the highest priority for all Best Effort traffic. This high priority reduces the latency of rtPS traffic under congestion.

With nrtPS, a service flow is created that provides a periodic opportunity for a cable modem to request permission to transmit data by polling a single cable modem for a bandwidth request, rather than all the cable modems. The data bursts may be of varying length. This kind of service flow is particularly suitable for non-interactive services such as file transfers.

Upstream Peak Traffic Rate

The Cisco uBR10012 universal broadband routers support upstream traffic peak rates (DOCSIS 3.0 TLV 24.27). This feature is supported on the Cisco uBR10012 universal broadband routers with the Cisco uBR10-MC5X20H and Cisco UBR-MC20X20V cable interface line cards and supports DOCSIS 2.0 and DOCSIS 3.0 cable modems. The upstream peak traffic rate is configured using the cable service class command. To view the peak traffic rate value for a specific service flow, use the **show cable modem qos verbose** and **show cable service-class verbose** commands.

Some of the DOCSIS 1.x and DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when they receive upstream peak rate TLV 24.27 from the Cisco CMTS. To overcome this, you can configure the **cable service attribute withhold-TLVs** command with **peak-rate** keyword to restrict sending of this type, length, value (TLV) to non-DOCSIS 3.0 cable modems.

Upstream Bandwidth Request Rate Limiting

The Cisco CMTS US scheduler may report high CPU consumption because of extensive incoming bandwidth request processing. The Cisco IOS Release 12.2(33)SCF introduces the upstream Bandwidth Request Rate Limiting (BRRL) feature, which controls the CPU consumption of the US scheduler by monitoring the number of incoming bandwidth requests, and dropping excessive bandwidth requests.

Note Only the best effort (BE) service flows are subjected to bandwidth request rate limiting.

By default, the BRRL feature is enabled for the Cisco uBR-MC3GX60V line card.

By default, all the bandwidth requests with service flow priority from 0 to 7 are processed by the BRRL feature. However, the BRRL feature also enables you to configure a service flow priority that is exempted from BRRL. Any bandwidth request received with this configured priority or above, is exempted from BRRL processing and is therefore not dropped even if the CPU consumption by the US scheduler is high. For example, if the configured exempted priority is 5, any bandwidth request with priority 5, 6, or 7 is not dropped even if the CPU consumption is high.

Use the **cable upstream rate-limit-bwreq exempted-priority** command to configure the exempted service flow priority. If the **exempted-priority** is set to value zero, all the bandwidth requests are exempted from rate limiting, or in other words BRRL feature is disabled.

How to Configure Upstream Scheduler Modes

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Use one the following commands: • **interface cable** *slot/subslot/port* • **interface cable** *slot/port* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 4	**cable upstream** *n* **scheduling type ugs mode** [**llq** |**docsis**] **Example:** `Router(config-if)# cable upstream 4 scheduling type ugs mode llq`	Enables LLQ-type (packet-based) scheduling for UGS services. **Note** Any combination of **ugs**, **rtps**, **nrtps**, **llq**, and **docsis** is allowed. The only default value is **docsis** .
Step 5	**cable upstream** *n* **scheduling type rtps mode** [**llq** |**docsis**] **Example:** `Router(config-if)# cable upstream 4 scheduling type rtps mode docsis`	Enables standard DOCSIS (TDM-based) scheduling for rtPS services. **Note** Any combination of **ugs**, **rtps**, **nrtps**, **llq**, and **docsis** is allowed. The only default value is **docsis** .
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

To confirm whether the scheduler is operating in LLQ or DOCSIS mode, use the **show interface cable mac-scheduler** command. A new queue is added when LLQ mode is enabled, as shown in the following example:

```
Router# show interface cable 4/0 mac-scheduler 0
     DOCSIS 1.1 MAC scheduler for Cable4/0/U0
     Queue[Rng Polls] 0/128, 0 drops, max 1
     Queue[CIR Grants] 0/64, 0 drops, max 0
     Queue[BE(7) Grants] 0/64, 0 drops, max 0
     Queue[BE(6) Grants] 0/64, 0 drops, max 0
     Queue[BE(5) Grants] 0/64, 0 drops, max 0
     Queue[BE(4) Grants] 0/64, 0 drops, max 0
     Queue[BE(3) Grants] 0/64, 0 drops, max 0
     Queue[BE(2) Grants] 0/64, 0 drops, max 0
     Queue[BE(1) Grants] 0/64, 0 drops, max 0
```

```
    Queue[BE(0) Grants] 0/64, 0 drops, max 0

  !This queue is added in LLQ Mode
  Queue[LLQ Grants] 0/64, 0 drops, max 0
     Req Slots 153607143, Req/Data Slots 0
     Init Mtn Slots 1305584, Stn Mtn Slots 145897
     Short Grant Slots 47, Long Grant Slots 2939
     ATDMA Short Grant Slots 0, ATDMA Long Grant Slots 0
     ATDMA UGS Grant Slots 0
     Awacs Slots 0
     Fragmentation count 3
     Fragmentation test disabled
     Avg upstream channel utilization : 0%
     Avg percent contention slots : 98%
     Avg percent initial ranging slots : 1%
     Avg percent minislots lost on late MAPs : 0%
     Sched Table Adm-State: Grants 0, Reqpolls 0, Util 1%
     UGS    : 0 SIDs, Reservation-level in bps 0
     UGS-AD : 0 SIDs, Reservation-level in bps 0
     RTPS   : 0 SIDs, Reservation-level in bps 0
     NRTPS  : 0 SIDs, Reservation-level in bps 0
     BE     : 2 SIDs, Reservation-level in bps 0
     r4k ticks in 1ms 131000
     Total scheduling events 0
     No search was needed 0
     Previous entry free 0
     Next entry free0
     Could not schedule 0
     Recovery failed 0
Curr time 8282 entry 90
```

How to Configure Exempted Priority for BRRL feature

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable upstream rate-limit-bwreq exempted-priority** *priority* **Example:** `Router(config)# cable upstream rate-limit-bwreq exempted-priority 5`	Configures the exempted priority: • *priority*—Service flow priority. Bandwidth requests with this service flow priority value (and above) are exempted from BRRL. The valid range is from 0 to 7.
Step 4	**end** **Example:** `Router(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Additional References

The following sections provide references related to the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco CMTS Cable Command Reference* http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

Standards

Standard	Title
DOCSIS	Data-Over-Cable Service Interface Specifications, DOCSIS 2.0, Radio Frequency Interface Specification, CM-SP-RFIv2.0-I08-050408

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Upstream Scheduler Mode for the Cisco CMTS Routers

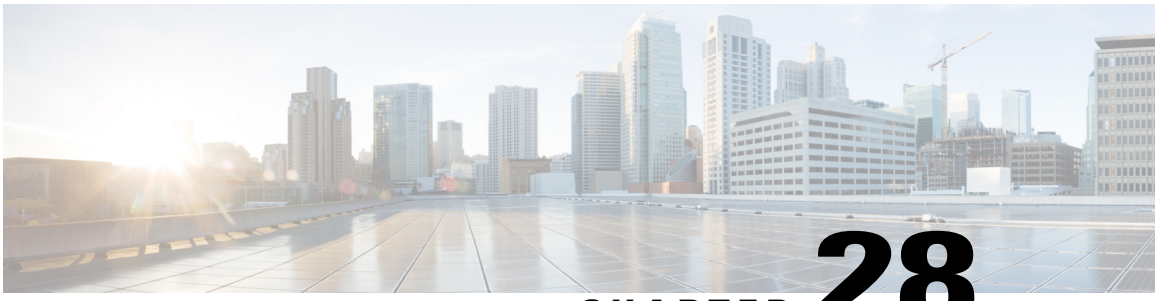
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 78: Feature Information for Upstream Scheduler Mode for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Upstream Scheduler Mode for the Cisco CMTS Routers	12.3(13)BC	This feature was introduced for all Cisco CMTS routers. The **cable upstream scheduling type** command was introduced.
Upstream Scheduler Mode for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR universal broadband router was added.
Upstream Peak Traffic Rate	12.2(33)SCC	The upstream peak rate traffic (DOCSIS 3.0 TLV 24.27) is supported on Cisco uBR10012 universal broadband routers. The following command outputs display the upstream peak traffic rate: • **show cable modem qos verbose** • **show cable service-class verbose**
Suppressing Downstream and Upstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems	12.2(33)SCB10	This featuer restricts sending of the DOCSIS 3.0 TLVs to DOCSIS 1.x and DOCSIS 2.0 cable modems. The **cable service attribute withhold-TLVs** command was introduced.

Feature Name	Releases	Feature Information
Upstream Bandwidth Request Rate Limiting	12.2(33)SCF	In the Cisco IOS Release 12.2(33)SCF, this feature was introduced for all Cisco CMTS routers. The **cable upstream rate-limit-bwreq exempted-priority** command was introduced.



CHAPTER 28

Upstream Utilization Optimization on the Cisco CMTS Routers

First Published: May 12, 2008

Last Updated: December 17, 2009

The Upstream Utilization Optimization feature on the Cisco Cable Modem Termination System (CMTS) provides higher upstream throughput.

Note Cisco IOS Release 12.2(33)SCB integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Upstream Utilization Optimization

You must have Advanced Time Division Multiple Access (A-TDMA)-capable line cards.

For optimum performance, do the following:

- Set the maximum upstream burst on the cable modem to a large number; for example, 28,000 bytes.
- Set the maximum concatenation burst on the cable modem to a large number; for example, 28,000 bytes.
- Set the cable modem upstream maximum traffic burst parameter to a large number (for example, zero means no limit) using the **cable default-phy-burst** command.

The Upstream Utilization Optimization feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table below shows the hardware compatibility prerequisites for this feature.

Table 79: Upstream Utilization Optimization Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(23)BC2 • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCB • PRE-2 • PRE-4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.3(23)BC2 • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCB • Cisco uBR10-MC5X20S/U/H
Cisco uBR7200 Series Universal Broadband Routers	Cisco IOS Release 12.3(23)BC2 • NPE-G1 Cisco IOS Release 12.2(33)SCB • NPE-G1 • NPE-G2	Cisco IOS Release 12.3(23)BC 2 • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCB • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCB • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCB • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Information about Upstream Utilization Optimization

Upstream utilization optimization provides the following benefits and functions on a Cisco CMTS router:

- Group configuration mode enables upstream utilization optimization eligibility on all cable modem upstream flows.
- Local configuration mode enables upstream utilization optimization eligibility on a specific upstream, provides configuration of selective parameters, and provides that local configuration overrides any global configuration.

How to Configure Upstream Utilization Optimization

The following tasks describe how to configure the Upstream Utilization Optimization feature:

Configuring Upstream Utilization Optimization Globally

By default, the Upstream Utilization Optimization feature is turned off. To globally enable upstream utilization optimization, use the **cable upstream rate-adapt** command in global configuration mode. All upstream flows created after this feature is enabled globally are eligible to rate-adapt. Using the **priority** or **rate** option allows you to restrict upstream utilization optimization to service flows that meet or exceed specified levels for priority or rate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable upstream rate-adapt** [**local** | **priority** *value* | **rate** *number*] **Example:** `Router(config)# cable upstream rate-adapt priority 6`	Enables upstream utilization optimization globally on all upstream flows. • **local—**(Optional) Enables upstream utilization optimization eligibility and configuration for a specific upstream flow. • **priority—**(Optional) Enables upstream utilization optimization on flows that meet or exceed a configured priority. The valid range is 0–7. • **rate—**(Optional) Enables upstream utilization optimization on flows that meet or exceed a specified minimum max-rate. The valid range is 0–30000000.

Configuring Upstream Utilization Optimization Locally Per Upstream

To configure a specific local upstream for upstream utilization optimization, use the **cable upstream rate-adapt** command in cable interface configuration mode for a specified upstream flow. You can configure several parameters for specific local upstream utilization optimization. By default, upstream utilization optimization uses the global configuration. However, when rate-adapt is configured on a local upstream, the local configuration parameters override the global configuration parameters.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** **Example:** `Router(config)#: interface cable 4/0/0`	Enters cable interface configuration mode.
Step 4	**cable upstream** *port* **rate-adapt** [**bcs** *slots* | **duration** *millisecs* | **fcms-off** | **priority** *value* | **rate** *number*] **Example:** `Router(config-if)# cable upstream 0 rate-adapt priority 6`	Enables upstream utilization optimization configuration on specific upstream flows. • **bcs—**(Optional) Specifies the number of broadcast contention minislots (BCS). MAPs that have gaps are filled with BCS. By default, 10 BCS slots are saved. You can override the default of 10 with a larger or smaller number. The valid range is 0–80. The default is 10.

	Command or Action	Purpose
		• **duration—**(Optional) Enables configuration of the duration of a flow rate-adapt in milliseconds. You can override the default of one second for rate-adapt grants to a flow. A larger or smaller duration can be chosen. The valid range is 0–2000. • **fcms-off—**(Optional) Enables an override to the default forced broadcast contention minislot that follows each filled MAP. By default, fcms is turned on. • **priority—**(Optional) Enables upstream utilization optimization on flows that meet or exceed a configured priority. This overrides a globally configured rate-adapt priority. The valid range is 0–7. • **rate—**(Optional) Enables upstream utilization optimization on flows that meet or exceed a specified minimum max-rate. This overrides a globally configured rate-adapt rate. The valid range is 0–30000000.

Verifying Upstream Utilization Optimization Configuration

To verify the cable upstream utilization optimization configuration for cable modem upstream, use the **show** commands described below.

- To display upstream utilization optimization parameters, use the **show cable rate-adapt** command as shown in the following example. Global upstream utilization optimization is enabled, local upstream utilization optimization is disabled. The duration is 500 and there is no rate or priority configured.

```
router# show cable rate-adapt
show_cable_rate-adapt_command: Global:Enabled Local-Only:Disabled
:maps 500 flags 0x1 priority -1, rate -1 bcs 10 fcms On
```

- To display the upstream utilization optimization settings and the parameters for a specific upstream, use the **show interface cable upstream** command as shown in the following example. On upstream 0, global and local upstream utilization optimization are enabled, the duration is 250, priority is 255, bcs is set to 0, rate is not configured, and the fcms feature is turned off.

```
router# show interface cable 8/0/0 upstream 0 rate-adapt
cmts_rate-adapt_show: Global:Enabled US[0]:Enabled
local:maps 250 pri 255, rate -1 bcs 0 (0) fcms Off
```

- To display service identifier (SID) and upstream utilization optimization information for a service flow, use the **show interface cable sid** command with the **counter** and **verbose** options as shown in the following example. On 8/0/0, upstream utilization optimization is enabled, 35542 rate-adapt requests were received, and there was one piggy-back request received from the upstream.

```
router# show interface cable 8/0/0 sid counters verbose
Sid : 1
Request polls issued : 0
BWReqs {Cont,Pigg,RPoll,Other} : 7, 146975, 0, 0
No grant buf BW request drops : 0
Rate exceeded BW request drops : 0
Grants issued : 1264300
Packets received : 2199040
Bytes received : 3241369899
rate-adapt : Enabled
```

```
rate-adapt {rcvd, Consec-PB} : 35542, 1
Fragment reassembly completed : N/A
Fragment reassembly incomplete : N/A
Concatenated packets received : N/A
Queue-indicator bit statistics : 0 set, 0 granted
Good Codewords rx : 14615740
Corrected Codewords rx : 1
Uncorrectable Codewords rx : 0
Concatenated headers received : 146807
Fragmentation headers received : 1296069
Fragmentation headers discarded: 240
```

Additional References

The following sections provide references related to the Upstream Utilization Optimization feature on the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cable commands	*Cisco IOS CMTS Cable Command Reference,* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Line card configuration information	• *Configuring the Cisco uBR10-MC5X20U/H Broadband Processing Engine* http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/feature/guide/mc5x20u.html
Software configuration information	• *Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/12_2sc/cbl_12_2sc_book.html • *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* (for Cisco IOS Release 12.3BC) http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html • *Cisco uBR7200 Series Software Configuration Guide* (for Cisco IOS Release 12.3BC) http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/configuration/guide/cr72scg.html

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

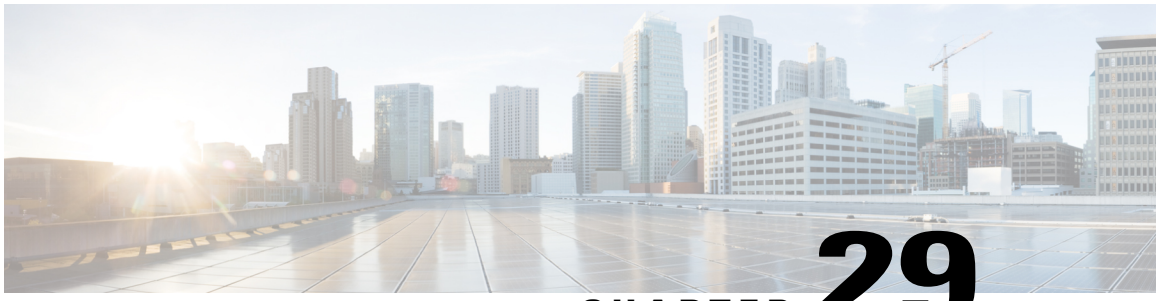
Feature Information for Upstream Utilization Optimization

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 80: Feature Information for Upstream Utilization Optimization

Feature Name	Releases	Feature Information
Upstream Utilization Optimization	12.3(23)BC2	This feature was introduced and provides increased upstream CM throughput. The following commands were introduced or modified: • **cable upstream rate-adapt (global)** • **cable upstream rate-adapt (interface)** • **show cable rate-adapt** • **show interface cable sid** • **show interface cable upstream**
Upstream Utilization Optimization	12.2(33)SCB	This feature was integrated into Cisco IOS Release 12.2(33)SCB.



CHAPTER 29

Wideband Modem Resiliency

First Published: December 17, 2008

Last Modified: January 20, 2013

The Wideband Modem Resiliency feature provides reliable service in the event of non-primary RF channel disruptions to ensure that a cable modem remains operational. With the implementation of this feature, the Cable Modem Termination System (CMTS) does not force a cable modem to perform a MAC reset if the cable modem loses connectivity to the CMTS on one or all of its non-primary RF channels.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Wideband Modem Resiliency

The table below shows the hardware compatibility prerequisites for the Wideband Modem Resiliency feature.

Table 81: Cable Hardware Compatibility Matrix for Wideband Modem Resiliency

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V
Cisco uBR7246VXR Universal Broadband Routers	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

Restrictions for Wideband Modem Resiliency

- This feature provides resiliency support only for downstream RF channel disruptions in Cisco IOS Release 12.2(33)SCB and later releases. This feature does not support any upstream-related resiliency.
- The CMTS cannot move a w-online cable modem to a bonding group that contains an RF channel that is not a member of the original Receive Channel Configuration (RCC) for the wideband cable modem.

Information About Wideband Modem Resiliency

The Wideband Modem Resiliency feature enables the Cisco uBR10012 or Cisco uBR7200 series router to interact with DOCSIS 3.0-compliant cable modems. This interaction helps provide reliable service in the event of non-primary channel disruptions of layer 1 and/or layer 2 connections, and loss of quadrature amplitude modulation (QAM) lock and/or MAC Domain Descriptor (MDD) timeout. If a cable modem loses connectivity with the CMTS on one or all of its non-primary RF channels, the CMTS does not force the cable modem to perform a MAC reset and enables the cable modem to remain operational.

A DOCSIS 3.0-qualified CMTS transmits data to one or more DOCSIS 3.0-compliant cable modems using multiple RF channels. For a cable modem, one of the RF channels is used as the primary RF channel, and the rest of the channels are considered non-primary channels. The primary RF channel is defined as the downstream (DS) RF channel on which the cable modem receives DOCSIS MAC messages needed for upstream timing and synchronization.

This feature enables the CMTS to collect and analyze data related to RF channel disruptions per cable modem to assist in identifying the impairment.

CM-STATUS Messages

Cable modems use CM-STATUS messages to report events to the CMTS. A DOCSIS 3.0-compliant cable modem does not perform a MAC reset when reporting DS RF channel failures through CM-STATUS messages. The CMTS does not send an acknowledgement to the cable modem when it receives a CM-STATUS message. The CMTS might not receive a CM-STATUS message, if the message gets corrupted during transmission. To prevent this occurrence, the CMTS sends the following two parameters to the cable modem using the primary MDD message for each event type:

- Maximum reports
- Maximum hold-off time

The maximum reports parameter specifies how many reports should be sent each time a particular event occurs. The maximum hold-off time parameter defines the amount of time (in units of 20 milliseconds) a cable modem should wait between transmissions of the CM-STATUS messages when the maximum reports parameter is greater than one.

RF Channel Event Dampening Time

The Wideband Modem Resiliency feature enables the CMTS to reduce the occurrence of a particular RF channel event by using the **cable rf-change-dampen-time** command. This command can also be used to prevent premature cable modem reconfiguration in the event of a prolonged outage. For example, the failover time of a remote edge-QAM device (EQAM) may be 10 seconds. Using the **cable rf-change-dampen-time** command, you can specify the dampening time such that an EQAM failover does not inadvertently trigger a mass reconfiguration of wideband cable modems.

Response of CMTS to RF Impairment Recovery

When cable modems report the recovery from downstream RF channel failures and their default downstream service flow has been moved to their primary downstream channel, the response of the CMTS is different between the following two Cisco IOS releases:

- Cisco IOS Release 12.2(33)SCB and later releases—If a cable modem reports that full service has been restored after downstream RF channel failures, the CMTS forces the cable modem to perform a MAC reset.
- Cisco IOS Release 12.2(33)SCC and later releases—If a cable modem reports that full service has been restored, the CMTS does not force the cable modem to perform a MAC reset, and the cable modem is kept w-online (the wideband downstream service is restored by the original wideband interface without a MAC reset).

Trigger Thresholds for Downstream Events

When a cable modem reports a downstream channel impairment via a CM-STATUS message, the cable modem can no longer reliably receive data on that channel. The Cisco CMTS must not use that channel to

transmit data to the cable modem. The Cisco CMTS uses the following three options to prevent the use of the impaired channel(s):

- Option 1—Suspend the RF channel(s) from the wideband interface used by that cable modem.
- Option 2—Move the default downstream service flow from its wideband interface to its primary channel interface (modular or cable).
- Option 3—Move all the downstream service flows (primary and unicast secondary service flows) from its wideband interface to its primary channel interface (modular or cable).

Choosing option 1 retains all the remaining operational DS channels active, option 2 retains only a single DS channel, and option 3 retains all DS channels. Option 1 affects all cable modems that are receiving service via the affected wideband interface, while options 2 and 3 only affect the cable modem reporting the impairment.

To control which option the Cisco CMTS uses when an RF impairment is reported, use the **cable rf-change-trigger** command. This command enables you to configure thresholds (percent and count) for an event before the event triggers an action for the cable modem. This command also enables you to configure a secondary keyword to move all the secondary downstream service flows of a cable modem to the primary channel interface.

Because the CM-STATUS messages are received sequentially, the decision to use options 1, 2, or 3 is made based on whether the trigger threshold is reached or not, and if the secondary keyword is configured. The table below lists the **cable rf-change-trigger** command conditions and the corresponding options selected by the Cisco CMTS.

Table 82: Conditions for Selecting RF Impairment Handling Options

rf-change-trigger Threshold Reached	secondary Keyword Configured	RF Impairment Handling Option Selected by the Cisco CMTS
YES	NA	Option 1
NO	NO	Option 2
NO	YES	Option 3

Note Before the rf-change-trigger count has reached, FrwdIF moves to the NB primary interface and only after the rf-change-trigger count has reached, FrwdIF moves to the WB interface. Do not move the previous FrwdIF from NB primary interface to WB Interface.

If the trigger thresholds for an event are not configured, the state of the non-primary RF channels always remains up, and the cable modems that report RF failures are reset after the dampening time specified in the **cable rf-change-dampen-time** command expires. If both thresholds are configured, then both the thresholds must be reached before changing the RF channel state to down.

In addition to not meeting the configured rf-change-trigger, a cable modem that reports impairments has its downstream service flows modified in option 2 or option 3, to provide reliable service in the following conditions:

- If the count exceeds the specified number of cable modems but the percent threshold is not reached.

- If the percent threshold is reached but the count does not reach the specified number of cable modems.
- If all non-primary channels of the cable modem are reported down.

Additionally with option 3, only those unicast secondary service flows (static or dynamic) which share the same wideband interface as the primary service flow, are moved to the primary channel interface (modular or cable). Any new dynamic service flows are created on the primary channel interface.

A suspended RF channel is restored for all affected wideband interfaces when a specified number of cable modems report (via CM-STATUS) that the channel connectivity is restored. The Wideband Modem Resiliency feature defines the specified number of cable modems as half of the configured count or percentage of rf-change-trigger, or both. For example, if the count is 20 and the percent is 10, then the number of cable modems reporting recovery should reduce the count to 10 and the percent to 5 for the suspended RF channel to be restored.

When either option 2 or option 3 is chosen by the Cisco CMTS, the service flows are not moved back to the original wideband interface until all the impaired RF channels are restored. However, with option 3 the *existing* dynamic secondary service flows, which are transitory in nature, are not moved back to the wideband interface even when all RF channels are restored.

The table below lists the various RF channel impairment handling options that the cable modem chooses and their applicable Cisco IOS releases.

Table 83: Release Specific Behavior for RF Impairment Handling options

RF Impairment Handling Options	Applicable Cisco IOS Releases
Option 1	Cisco IOS Release 12.2(33)SCB and later releases.
Option 2	Cisco IOS Release 12.2(33)SCC and later releases.
Option 3	Default behavior in Cisco IOS Release 12.2(33)SCB and SCB-based releases. All downstream service flows (primary or secondary) are moved to primary channel interface. Configurable behavior in Cisco IOS Release 12.2(33)SCE4 and later releases. The decision to move all secondary service flows can be configured using the **cable rf-change-trigger** command. For more information, see the *Cisco IOS CMTS Cable Command Reference* guide.

How to Configure Wideband Modem Resiliency

The following tasks describe how to configure the Wideband Modem Resiliency feature on a Cisco uBR10012 or Cisco uBR7200 series router:

Specifying Trigger Thresholds for Downstream Events

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rf-change-trigger [percent** *value***] [count** *number***] [secondary]** **Example:** `Router(config)# cable rf-change-trigger percent 50 count 1 secondary`	Specifies the amount of time an event must persist before it triggers an action for the reporting cable modem. • **percent** *value*—(Optional) Indicates the percentage of cable modems that must report that a particular non-primary RF channel is down before that channel is removed from the bonding group with that NP RF channel configured. The valid range is from 1 to 100. The default value is 0. • **count** *number*—(Optional) Specifies the number of cable modems reporting an impairment for a non-primary downstream channel. The default value is 0. • **secondary—**(Optional) Configures the Cisco CMTS to move the unicast secondary service flows to primary interface, when the number of cable modems reporting RF channel impairment is less than the configured (percent or count) threshold. **Note** Only those unicast secondary service flows, which share the same wideband interface as the primary interface, are moved to the primary channel interface.

Specifying Persistence Time for RF Channels

To configure the amount of time a non-primary RF channel must remain in its current state (either up or down), use the **cable rf-change-dampen-time** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable rf-change-dampen-time** *seconds* **Example:** `Router(config)# cable rf-change-dampen-time 10`	Specifies the amount of time in seconds for a non-primary RF channel to remain in its new state. The default value is 30.

Changing Default CM-STATUS Configuration

To change the default configuration values of "Event Holdoff Timer" and "Number of Reports per Event" for any or all events, use the **cable cm-status** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable cm-status** {**all** | *event*} [**holdoff** {*timer* | **default**} | **reports** {*reportvalue* | **default**}] **Example:** `Router(config-if)# cable cm-status 1 holdoff 1`	Sets the holdoff timer (in units of 20 milliseconds) and the number of reports per event value. • *event*—CM-STATUS event. The valid range is from 1 to 10. • *timer*—Holdoff timer value. The valid range is from 1 to 65535. The default value is 50. • *reportvalue*—Report value. The valid range is from 0 to 255. The default value is 2.

Verifying Wideband Modem Resiliency

Use the following **show** commands to verify the state of RF channels and the other configuration details:

- **show interface rf-status**
- **show cable rf-status**
- **show cable modem wideband rcs-status**
- **show cable modem**

To verify the logical up and down state for each of the configured RF channels for a wideband interface, use the **show interface rf-status** command as shown in the following example:

Cisco uBR10012 Universal Broadband Router:

```
Router# show interface wideband-cable 1/0/0:3 rf-status
 Logical
RF  Status
--  ------
17  UP
18  UP
19  UP
```

Cisco uBR7200 Series Universal Broadband Router:

```
Router# show interface wideband-cable 5/1:0 rf-status
            Logical
Resource    RF  Status
----------------------
5/1         0   UP
            1   UP
            2   UP
```

To verify the logical up and down state of the specified channel number, or the logical state of all RF channels, use the **show cable rf-status** command as shown in the following example:

```
Router# show cable rf-status
          Logical  Flap    Flap
RF        Status   Counts  Time
--------  -------  ------  ----
1/0/0 0   UP       0
      1   UP       0
      2   UP       0
      3   UP       0
      5   UP       0
      6   UP       0
      7   UP       0
      8   UP       0
      9   UP       0
      10  UP       0
      11  UP       0
      12  UP       0
      13  UP       0
      14  UP       0
      15  UP       0
      16  UP       0
```

To verify details of events for each RF channel in the cable modem's Receive Channel Configuration (RCC), use the **show cable modem wideband rcs-status** command as shown in the following example:

```
Router# show cable modem 0019.474a.c0ba wideband rcs-status
CM  : 0019.474a.c0ba
RF  : 1/0/0 10
```

```
  Status                    : UP
  FEC/QAM Failure           : 0
  Dup FEC/QAM Failure       : 0
  FEC/QAM Recovery          : 0
  Dup FEC/QAM Recovery      : 0
  MDD Failure               : 0
  Dup MDD Failure           : 0
  MDD Recovery              : 0
  Dup MDD Recovery          : 0
  Flaps                     : 0
  Flap Duration             : 00:00
RF  : 1/0/0 11
  Status                    : UP
  FEC/QAM Failure           : 0
  Dup FEC/QAM Failure       : 0
  FEC/QAM Recovery          : 0
  Dup FEC/QAM Recovery      : 0
  MDD Failure               : 0
  Dup MDD Failure           : 0
  MDD Recovery              : 0
  Dup MDD Recovery          : 0
  Flaps                     : 0
  Flap Duration             : 00:00
```

To verify the basic receive statistics for all possible event code types for the specified cable modem, use the **show cable modem** command as shown in the following example:

```
Router# show cable modem cm-status
I/F    MAC Address    Event            TID   Count Error Dups  Time
C7/0   001c.ea2b.79b2 MDD timeout      0     0     1     0     Jan 11 11:29:22
                      QAM failure      0     0     1     0     Jan 11 11:29:02
                      MDD recovery     0     0     1     0     Jan 11 11:30:20
                      QAM recovery     0     0     1     0     Jan 11 11:30:13
C7/0   001c.ea2b.78b0 MDD timeout      0     0     1     0     Jan 11 11:29:16
                      QAM failure      0     0     1     0     Jan 11 11:28:53
                      MDD recovery     0     0     1     0     Jan 11 11:29:59
                      QAM recovery     0     0     1     0     Jan 11 11:29:46
Router# show cable modem 001c.ea2b.79b2 cm-status
I/F    MAC Address    Event            TID   Count Error Dups  Time
C7/0   001c.ea2b.79b2 MDD timeout      0     0     1     0     Jan 11 11:29:22
                      QAM failure      0     0     1     0     Jan 11 11:29:02
                      MDD recovery     0     0     1     0     Jan 11 11:30:20
                      QAM recovery     0     0     1     0     Jan 11 11:30:13
Router# show cable modem cable 7/0 cm-status
I/F    MAC Address    Event            TID   Count Error Dups  Time
C7/0   001c.ea2b.79b2 MDD timeout      0     0     1     0     Jan 11 11:29:22
                      QAM failure      0     0     1     0     Jan 11 11:29:02
                      MDD recovery     0     0     1     0     Jan 11 11:30:20
                      QAM recovery     0     0     1     0     Jan 11 11:30:13
C7/0   001c.ea2b.78b0 MDD timeout      0     0     1     0     Jan 11 11:29:16
                      QAM failure      0     0     1     0     Jan 11 11:28:53
                      MDD recovery     0     0     1     0     Jan 11 11:29:59
                      QAM recovery     0     0     1     0     Jan 11 11:29:46
```

What to Do Next

To modify the default configuration of events for CM-STATUS reports, proceed to the Modifying CM-STATUS Reports for Events, on page 733.

Modifying CM-STATUS Reports for Events

You can enable or modify the following ten CM-STATUS events per interface using the **cable cm-status enable** command:

- Secondary channel MDD time-out

- QAM/FEC lock failure
- Sequence out of range
- MDD recovery
- QAM/FEC lock recovery
- T4 time-out
- T3 re-tries exceeded
- Successful ranging after T3 re-tries exceeded
- CM operating on battery backup
- CM returned to A/C power

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable {slot/port |** *slot/subslot/port}* **Example:** `Router(config)# interface cable8/0/0`	Specifies the cable interface line card on a Cisco CMTS router: • *slot*—Chassis slot number of the cable interface line card. ◦ Cisco uBR7246VXR router: The valid range is from 3 to 6. ◦ Cisco uBR7225VXR router: The valid range is from 1 to 2. ◦ Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. ◦ Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. ◦ Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface).

	Command or Action	Purpose
Step 4	**cable cm-status enable** *range* **Example:** `Router(config-if)# cable cm-status enable 6-9`	Enables a particular CM-STATUS event on a primary cable interface. The valid range is from 1 to 10. The following events are enabled by default on cable and modular cable interfaces: • Secondary channel MDD time-out • QAM/FEC lock failure • Sequence out of range • MDD recovery • QAM/FEC lock recovery To disable a CM-STATUS event, use the **no** form of the **cable cm-status enable** command.

Enabling SNMP Traps for Wideband Resiliency Events

You can enable Simple Network Management Protocol (SNMP) traps for Wideband Resiliency specific events using the **snmp-server enable traps docsis-resil** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps docsis-resil** [*resil-events*] **Example:** `Router(config)# snmp-server enable traps docsis-resil rf-up`	Enables SNMP traps for wideband resiliency specific events. Traps can be sent for specific events using the *resil-events* option: • **cm-pmode—**Enables the wideband resiliency cable modem partial service trap. • **cm-recover—**Enables the wideband resiliency cable modem full service trap. • **event—**Enables the wideband resiliency event trap. • **rf-down—**Enables the wideband resiliency RF channel down status trap.

	Command or Action	Purpose
		• **rf-up—**Enables the wideband resiliency RF channel up status trap. To disable sending of the trap, use the **no** form of this command.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Enabling Wideband Resiliency Trap Notifications

You can enable Wideband Resiliency trap notifications to a specific SNMP host using the **snmp-server host traps docsis-resil** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *ipaddr* **traps** *string* **docsis-resil** **Example:** `Router(config)# snmp-server host 172.17.2.0 traps snmphost01 docsis-resil`	Enables wideband resiliency traps for a specific SNMP host. • *ipaddr*—IPv4 or IPv6 address of the SNMP notification host. • *string*—SNMPv1 community string, SNMPv2c community string, or SNMPv3 username. To disable, use the **no** form of this command.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Setting the Trap Interval

You can set the interval at which traps must be sent for Wideband Resiliency related events for each cable modem using the **cable resiliency traps-interval** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable resiliency traps-interval** *count* **Example:** `Router(config)# cable resiliency traps-interval 0`	Sets the time interval at which traps must be sent for each cable modem. • *count*—Time interval (in seconds) at which the traps must be sent for each cable modem. The valid range is from 0 to 86400. The default value is 1. To disable, use the **no** form of this command.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuration Example for Wideband Modem Resiliency

The following example shows how to configure the Wideband Modem Resiliency feature by specifying the dampening time and persistence thresholds for non-primary RF channels:

```
Router# configure terminal
Router(config)# cable rf-change-dampen-time 40
Router(config)# cable rf-change-trigger percent 50 count 1
Router(config)# cable cm-status 1 holdoff 1
```

Additional References

The following sections provide references related to the Wideband Modem Resiliency feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband) routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco DOCSIS 3.0 Downstream Solution	*Cisco DOCSIS 3.0 Downstream Solution Design and Implementation Guide* http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_2.0/ds_solu.html
Cisco Cable Wideband Solution Design	*Cisco Cable Wideband Solution Design and Implementation Guide* http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_1.0/wb_solu.html

Standards

Standard	Title
CM-SP-MULPIv3.0-I08-080522	DOCSIS 3.0 MAC and Upper Layer Protocol Interface Specification

MIBs

MIB	MIBs Link
CISCO-DOCS-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Wideband Modem Resiliency

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 84: Feature Information for Wideband Modem Resiliency

Feature Name	Releases	Feature Information
Wideband Modem Resiliency	12.2(33)SCB	The Wideband Modem Resiliency feature provides the best possible service in the event of non-primary RF channel disruptions. The following sections provide information about this feature: • How to Configure Wideband Modem Resiliency, on page 729 • Configuration Example for Wideband Modem Resiliency, on page 737 The following commands were introduced or modified: • **cable rf-change-dampen-time** • **cable rf-change-trigger** • **cable cm-status enable** • **show interface rf-status** • **show cable rf-status** • **show cable modem wideband rcs-status** • **show cable modem summary wb-rf** • **clear cable modem cm-status** • **clear cable modem rcs-counts** • **clear cable rf-status** • **debug cable wbcmts resiliency** • **show cable flap-list wb-rf**

Feature Name	Releases	Feature Information
Bypass the 24 Hour Timer for Wideband Cable Modems	12.2(33)SCB	This feature removes the 24-hour timer required to clear these channels. Once the cable modem successfully completes registration, the list of failed RF channels for that cable modem is cleared. If the RF impairment has been eliminated when the cable modem re-registers, that channel can be reused immediately. There are no new or modified commands for this feature.
Wideband Modem Resiliency	12.2(33)SCD	In Cisco IOS Release 12.2(33)SCD, this feature was introduced on the Cisco uBR7225VXR and Cisco uBR7246VXR routers. The following commands were introduced or modified: • **interface cable** • **show interface rf-status** • **show cable modem** • **clear cable modem cm-status** • **cable cm-status**
Move Secondary Service Flows to Primary Channel Interface.	12.2(33)SCE4	This feature enables the Cisco CMTS to move all the unicast secondary service flows to the primary channel interface, when the number of cable modems reporting the RF-channel impairment is less than the configured trigger threshold. For more information on this feature, see section Specifying Trigger Thresholds for Downstream Events, on page 730. The **cable rf-change-trigger** command was modified.

Feature Name	Releases	Feature Information
Downstream Wideband Resiliency Trap	12.2(33)SCG2	This feature enables SNMP traps for Wideband Resiliency related events and setting of the trap interval. For more information, see: • Enabling SNMP Traps for Wideband Resiliency Events, on page 735 • Enabling Wideband Resiliency Trap Notifications, on page 736 • Setting the Trap Interval, on page 737 The following commands were introduced or modified: • **cable resiliency traps-interval** • **snmp-server enable traps docsis-resil** • **snmp-server host traps docsis-resil**

PART IV

High Availability Features

CHAPTER 30

Cisco IOS In-Service Software Upgrade Process

First Published: December 17, 2008

Last Updated: July 11, 2012

The In-Service Software Upgrade (ISSU) process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU topics and describes the steps taken to perform ISSU in a system.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

- Feature Information for ISSU, page 795

Prerequisites for Performing ISSU

General Prerequisites

- Ensure that both the active and the standby Route Processors (RPs) are available in the system.
- The new and old Cisco IOS software images must exist in the file systems of both the active and standby RPs, and they both must have the same running image path, before you begin the ISSU process.
- ISSU is supported within a Cisco IOS Release. Upgrading between two different Cisco IOS Releases using ISSU process is not supported. For example, upgrading from Cisco IOS Release 12.2(33)SCG to Cisco IOS Release 12.2(33)SCH using ISSU is not supported.
- Stateful Switchover (SSO) must be configured and working properly. If you do not have SSO enabled, see the *Stateful Switchover* document for further information on how to enable and configure SSO.
- Nonstop Forwarding (NSF) must be configured and working properly. If you do not have NSF enabled, see the *Cisco Nonstop Forwarding* document for further information on how to enable and configure SSO. NSF must be configured on routers that are connected to the uBR broadband routers.

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 85: ISSU Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [53]

53 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Note Line card HA is supported for Cisco uBR-MC3GX60V line cards from 12.2(33)SCE1 onwards. ISSU is supported between rebuilds in the same release train. For example: ISSU is supported when upgrading from Cisco IOS Release 12.2(33)SCH FCS to Cisco IOS Release 2.2(33)SCH1.

Cisco uBR10012 Universal Broadband Router Platform Prerequisites

- The following WAN line card supports ISSU-uBR10K:
  - 1-Port Half-Height Gigabit Ethernet
- For the RLC ISSU process to run on cable line cards, the cable line cards must be configured for N+1 line card redundancy.

For more information about configuring N+1 redundancy, see N+1 Redundancy for the Cisco CMTS Routers .

Note If a cable line card is not configured for N+1 line card redundancy, it will be reloaded upon execution of the RP **issu linecard reloadversion** command. This will cause interruption of data service.

- The following jacket cards and SPA support Minimum Disruptive Restart (MDR):
  - Cisco 10000-SIP-600 Jacket card
  - SPA-24XDS-SFP (Wideband DOCSIS SPA)

Please see MDR Support for ISSU, on page 765 for more details.

- Before running any ISSU process, determine the compatibility level between the Cisco IOS software versions on the active and the standby RPs.
- The Dynamic Image Version Compatibility (DIVC) feature is not supported by the ISSU-uBR10K feature. The bundled compatibility matrix in the released image checks for the image compatibility. For more information, see the How to Perform the RP ISSU Process, on page 767.
- The ISSU process shall be performed under normal PRE CPU utilization and line card CPU utilization conditions. The ISSU process is not recommended when the PRE processor module CPU utilization is constantly higher than 80% or line card CPU utilization is higher than 90%.

High CPU consumption processes (such as SNMP polling) should be avoided during the ISSU process.

The following commands are used to check the PRE processor module CPU utilization and line card CPU utilization respectively prior to start of the ISSU process:

- **show processes cpu**
- **show controllers cable [proc-cpu]**

Restrictions for Performing ISSU

General Restrictions

- Before you perform ISSU, ensure the system is configured for redundancy mode SSO and that the file system for both the active and standby RPs contains the new ISSU-compatible image. The current version running in the system must also support ISSU. You can issue various commands to determine RP versioning and compatibility, or you can use the ISSU application on Cisco Feature Navigator.
- Do not make any hardware changes while performing an ISSU process.
- ISSU requires that there are no error conditions in the chassis. A Cisco UBR-MC20X20V cable interface line card in maintenance mode is considered an error condition. Upgrade the line card to a valid license or remove the maintenance mode line card from the system before performing ISSU.

Note ISSU supports only software upgrade on routers with the same PRE hardware. ISSU can be performed either on routers with dual PRE2 hardware or dual PRE4 hardware. ISSU does not support hardware upgrade of PRE2 to PRE4 or vice versa.

- ISSU operations utilize large amounts of system resources to perform reliable upgrades. Therefore, it is recommended that any unnecessary activities, such as excessive diagnostic activities like debugs, are ceased during all ISSU operations. However, the following debug commands do not adversely affect ISSU operations:
  - debug issu process
  - debug issu rlc-issu
  - debug cable preso
  - debug hccp timing
  - debug ipc issu

Note Usage of any other debug command during ISSU operations, apart from the ones specified above, may produce unexpected performance or results.

Cisco uBR10012 Universal Broadband Router Platform Restrictions

- ISSU-uBR10K process is available only in Cisco IOS Release 12.2(5th)SB and later on the Cisco uBR10012 Universal Broadband Router for the Performance Routing Engines- PRE-2 and PRE-4.
- The Cisco uBR10012 router supports ISSU processes at both the route processor (RP) level (for the PRE-2 cards), and at the line card (LC) level, with the following restrictions:
  - The RP ISSU process performs Minimal Disruptive Restart (MDR) functions for the supported WAN line cards, which supports a restart of the line card software with its associated upgraded or downgraded image, with minimum interruption of traffic flow.

Note The following WAN line cards support MDR for ISSU-uBR10K: 1-Port Half-Height Gigabit Ethernet and 10000-SIP-600 (4 bay Cisco 10000 SPA Jacket Card).

- The redundant LC (RLC) ISSU process does not run automatically as part of the RP ISSU process for cable line cards. The RLC ISSU process must be initiated manually for supported cable line cards.
- The RP ISSU process must be run prior to initiating the RLC ISSU process for the cable line cards. The RP must remain in the Run Version state until the RLC ISSU process completes while the standby RP must also be in hot standby, and ISSU accept version must have been run.
- If a cable line card is not configured for N+1 line card redundancy, you need to upgrade via a sequential reload, using the issu linecard reloadversion command. This will cause interruption of data service for the cable line card.

- The Dynamic Image Version Compatibility (DIVC) feature is not supported by the ISSU-uBR10K feature.
- While performing ISSU within a Cisco IOS Release (for example, Cisco IOS Release 12.2(33)SCH to Cisco IOS Release 12.2(33)SCH1), MIBs like CISCO-PROCESS-MIB cannot be accessed during the period between ISSU run version and accept version.

Information About Performing ISSU

Before you perform ISSU, you should understand the following concepts:

ISSU-uBR10K Process Overview

The ISSU-uBR10K feature enhances the set of High Availability (HA) features on the Cisco uBR10012 Universal Broadband Router by providing software upgrade or downgrade services for Cisco IOS software images and line card images on redundant Cisco uBR10012 router hardware, with minimal interruption of service. ISSU-uBR10K includes RP ISSU support between Performance Routing Engines and MDR support for certain WAN line cards, and extends the ISSU process to cable line cards.

On the Cisco uBR10012 router, the ISSU-uBR10K process consists of two phases:

1. RP ISSU phase—In this first phase, the RP ISSU process upgrades the image on the standby PREs and upgrades images for any supported WAN line cards with minimal network interruption.
2. RLC ISSU phase—(Supported only on the Cisco uBR10012 router) Once the RP ISSU process has been run and the RP is in the runversion state, this second ISSU phase can be initiated to upgrade images on redundant cable line cards. The other conditions to run the RP ISSU are standby RP has to be in hot standby mode and rollback timer has to be stopped using the issu acceptversion command.

If a cable line card is not configured for N+1 line card redundancy, you need to upgrade via a sequential reload, using the issu linecard reloadversion command.This will cause interruption of data service for the cable line card.

Switchovers during both the RP and RLC ISSU processes ensure that there are no cable modem drops (CMs do not go offline) and no PacketCable voice call drops.

RPU-only ISSU Process Overview

Existing Upgrade Process

The existing upgrade bundle consists two phases:

1. RP ISSU Upgrade: The RP ISSU upgrade is initiated. When the process reaches the issu runversion state, the RP rollback timer is stopped with **issu acceptversion** command.
2. Redundant LC ISSU Upgrade: The second phase is where the line cards connect to th new RPs and ISSU image negotiation begins. At this point, the **issu linecard** commands are executed one by one upto the **issu linecard runversion** command stage. The **issu commitversion** command is commonly executed for both RPs and line cards.

The RP-only ISSU Solution

This solution provides for upgrade of only the RP images without upgrading the line card images.

The RP-only ISSU process skips the Redundant LC ISSU Upgrade phase if the line card images matches the previous or old line card image bundled into the upgrade image. The Redundant LC ISSU Upgrade process is optional if the new upgrade image is an RP-only ISSU image.

1. The upgrade bundle must bundle the old LC image.
2. At present this process is supported only for Cisco uBR-MC20X20V and Cisco uBR-MC3GX60V line cards.

RP-only ISSU process uses the same commands that are used in the existing ISSU Upgrade process. The process consists the following steps:

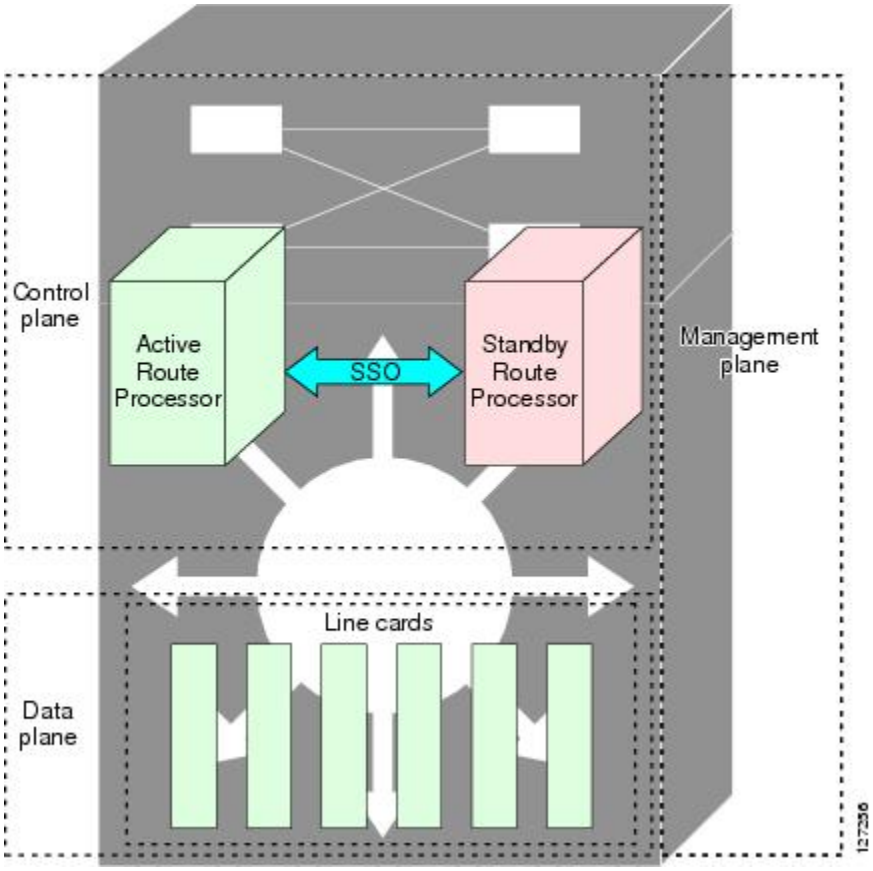
1. The RP-only ISSU Upgrade may be done using the ISSU Multi-Step Upgrade Process, page 24 or the ISSU Single-Step Upgrade Process, page 29.
2. 2.If the Multi-Step Upgrade process is used, the Redudndant LC ISSU process may be performed using the Running the RLC ISSU Process Automatically, page 36. The RLC ISSU upgrade process may be ignored if it is ensured that the upgrade image used for the ISSU Upgrade process is an RP-only ISSU image.
3. The upgrade must be completed using the t_Finishing_the_ISSU_Process_to_Enable_the_New_Cisco_IOS_Software_Version_on_the_RP_and_Cable_Line_Cards_1093719.xml#task_1093719.

RP ISSU Process Overview

The RP ISSU process allows you to perform a Cisco IOS software upgrade or downgrade while the system continues to forward packets. Cisco IOS ISSU takes advantage of the Cisco IOS high availability infrastructure—Cisco NSF with SSO and hardware redundancy—and eliminates downtime associated with software upgrades or version changes by allowing changes while the system remains in service (see Figure below). Cisco IOS software high availability features combine to lower the impact that planned maintenance activities have on network service availability, with the results of less downtime and better access to critical systems.

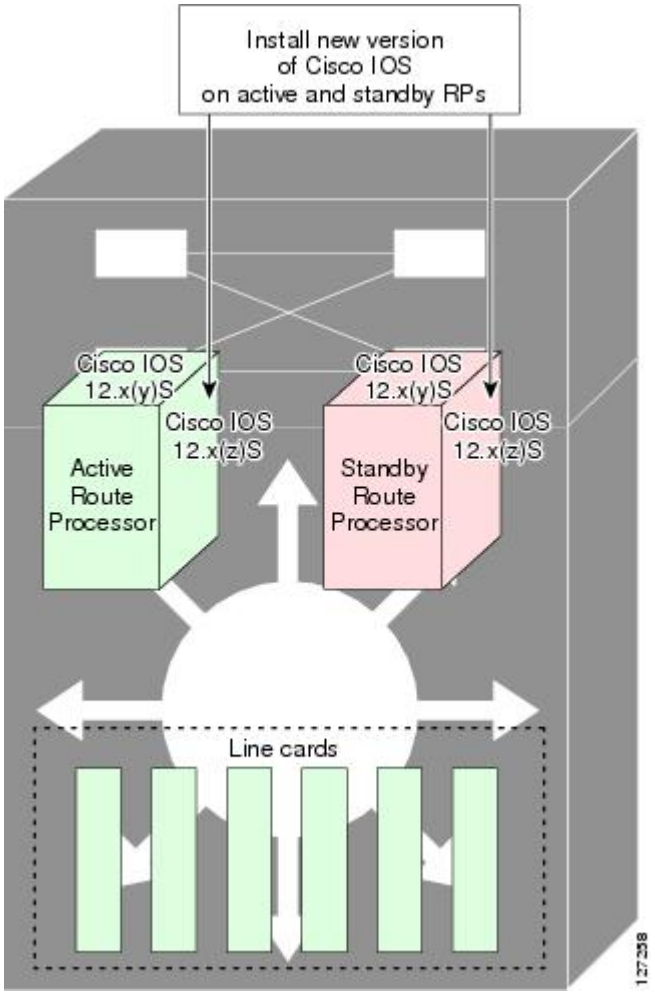
SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two RPs to be kept in synchronization although they may support different sets of commands.

Figure 9: High Availability Features and Hardware Redundancy in the ISSU Process



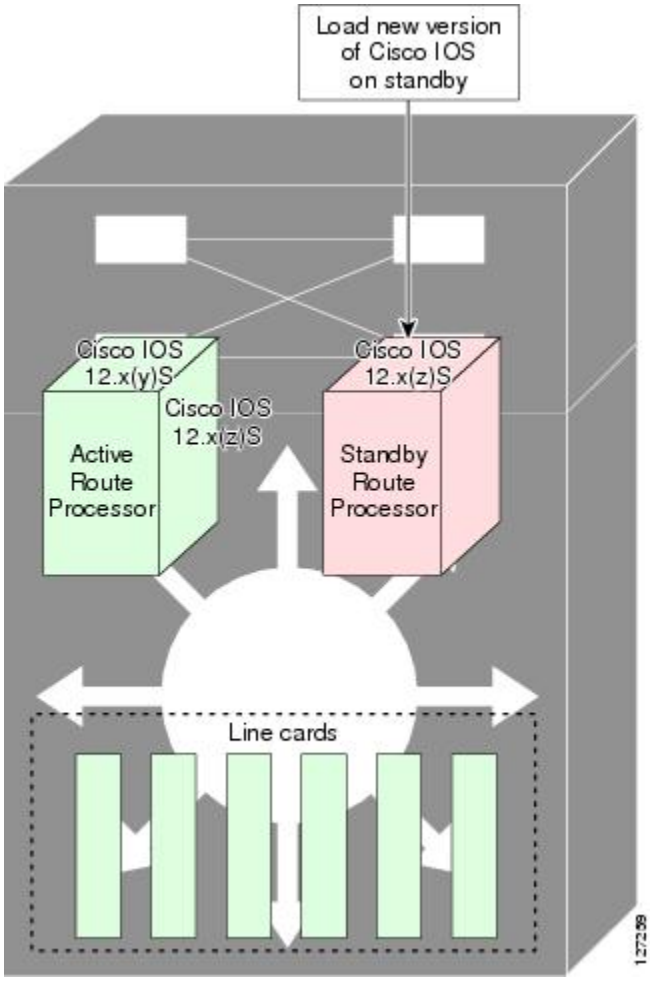
An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, copy the Cisco IOS software into the file systems of both RPs (see Figure below).

Figure 10: How to Load New Cisco IOS Software on Both RPs



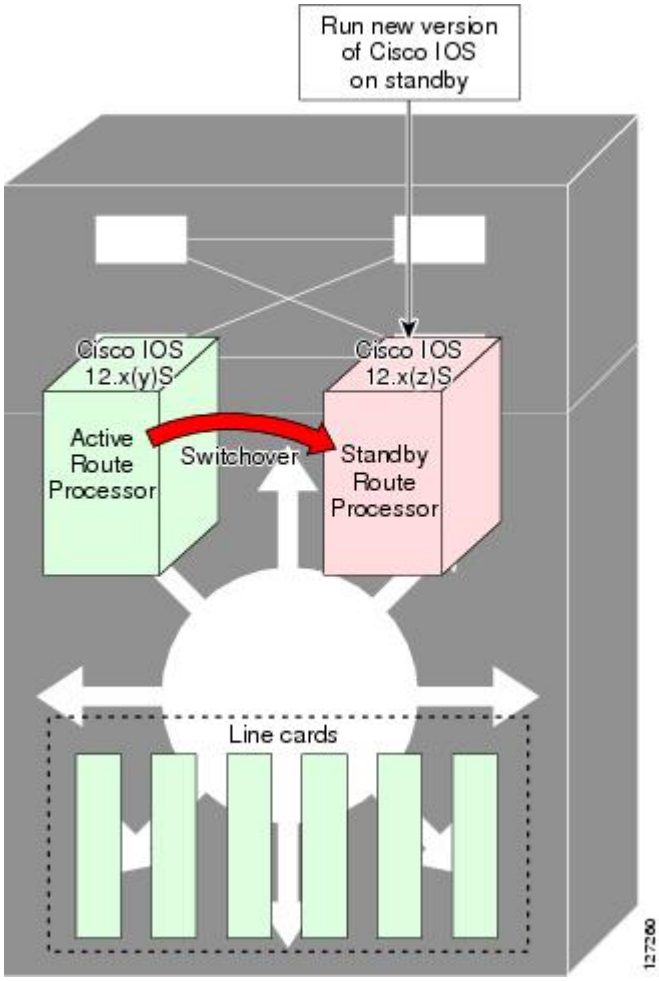
After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP (see Figure below).

Figure 11: Load New Cisco IOS Software on the Standby RP



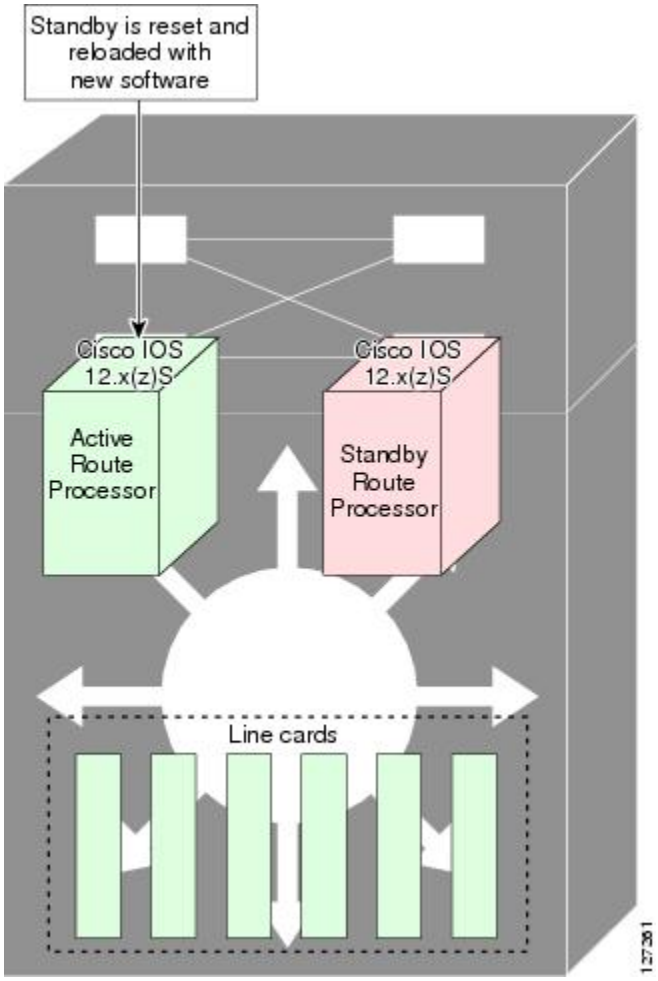
After switchover, the standby RP takes over as the new active RP (see Figure below).

Figure 12: Switch Over to Standby RP



Then, the former active RP, which is now the new standby RP, is loaded with the new software (see Figure below).

Figure 13: Load New Standby RP with New Cisco IOS Software

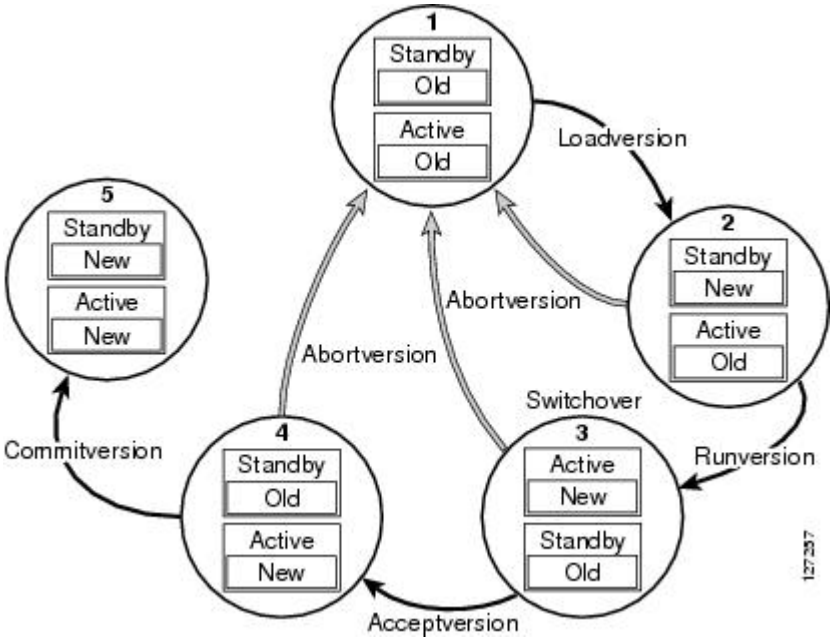


The two RPs in a system can be in one of three different states during ISSU:

- Active—One RP is actively forwarding packets with old software. After the ISSU process is performed, the original active RP becomes the standby RP.
- Standby—Perform ISSU on the standby RP, loading it with new software. After the ISSU process is performed, the original standby RP is the new active RP.
- Hot standby—After the original standby RP becomes the new active RP, load the new software image into the new standby RP. Doing so makes the standby RP a hot standby RP.

Figure below shows the ISSU states during the ISSU process.

Figure 14: ISSU States During the ISSU Process



Stateful Switchover Overview

Development of the SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

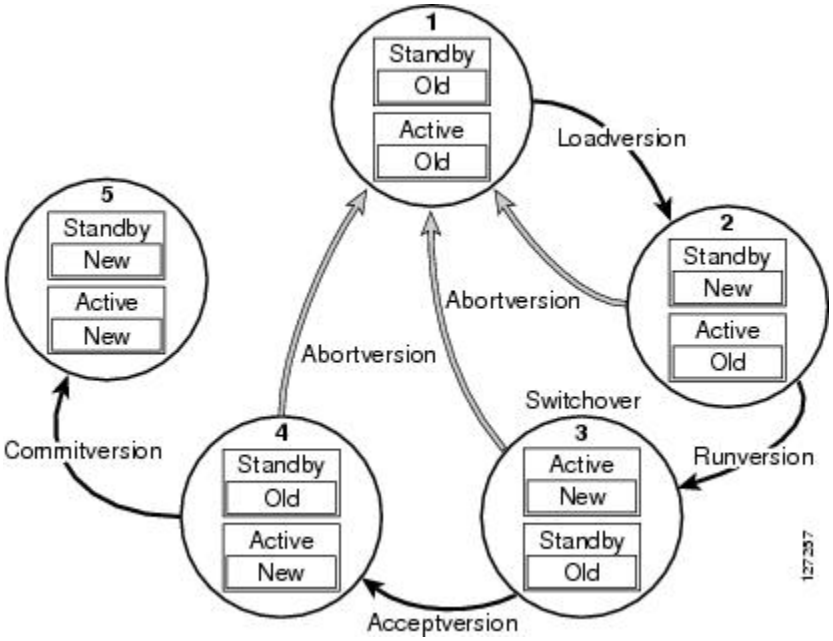
Cisco NSF is used with SSO. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, thereby reducing loss of service outages for customers.

Figure below illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is enabled at the access layer (edge) of the service provider network. A fault at this point could result in loss of service for enterprise customers requiring access to the service provider network.

For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Depending on your objectives,

you may decide to deploy Cisco NSF and SSO features at the core layer of your network. Doing this can help reduce the time to restore network capacity and service for certain failures, which leads to additional availability.

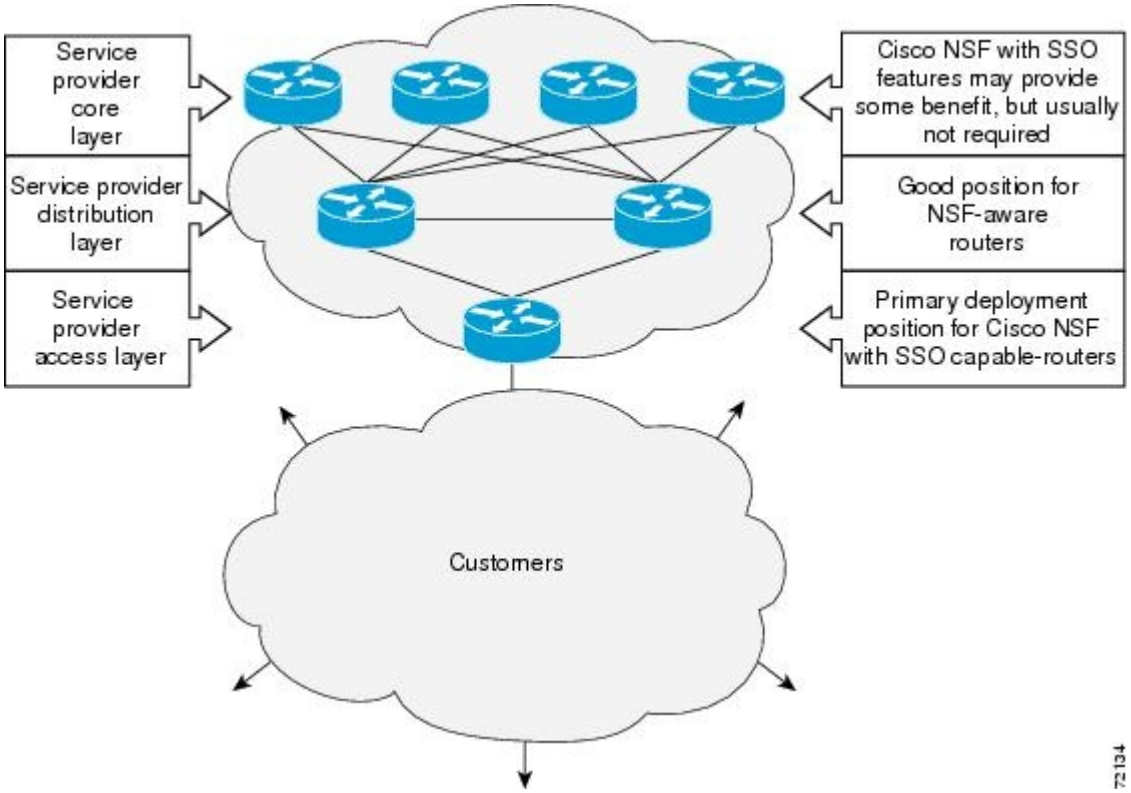
Figure 15: Cisco NSF with SSO Network Deployment: Service Provider Networks



Additional levels of availability may be gained by deploying Cisco NSF with SSO at other points in the network where a single point of failure exists. Figure below illustrates an optional deployment strategy that applies Cisco NSF with SSO at the enterprise network access layer. In this example, each access point in the

enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Figure 16: Cisco NSF with SSO Network Deployment: Enterprise Networks



For further information on SSO, see the Stateful Switchover document.

NSF Overview

Cisco NSF works with the SSO feature in Cisco IOS software. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco NSF is to continue forwarding IP packets following an RP switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to Cisco NSF operation.

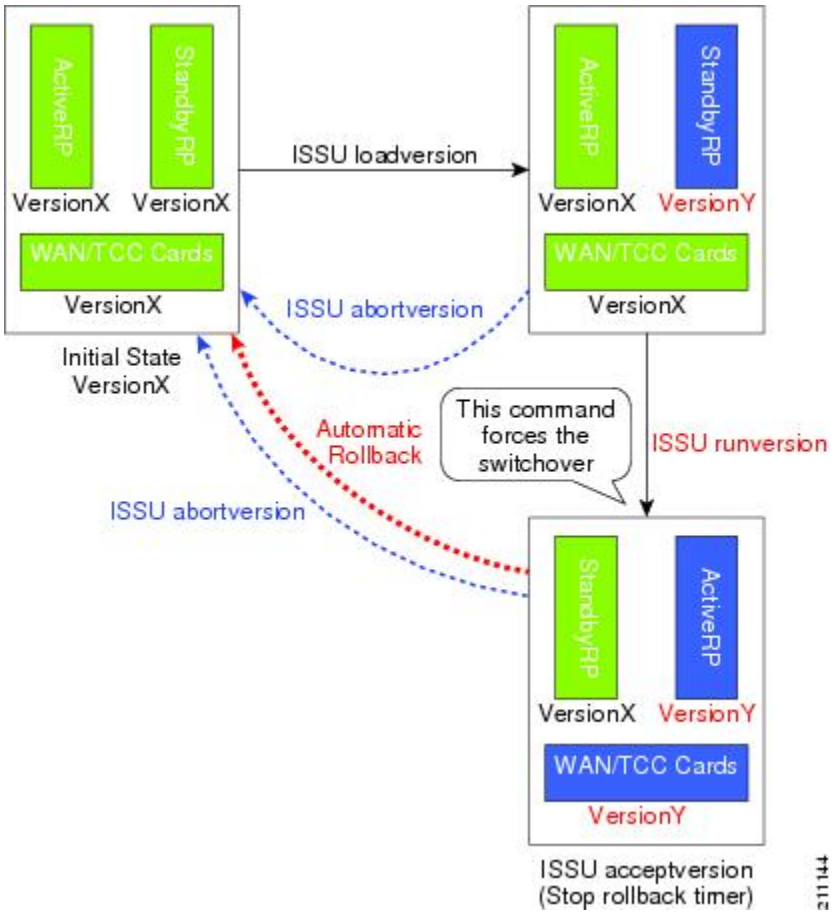
Redundant LC ISSU Process Overview

Note Effective with Cisco IOS Release 12.2(33)SCH2, in the RP-only ISSU process, the Redundant LC ISSU Upgrade process is optional.

The redundant LC (RLC) ISSU process is introduced in Cisco IOS Release 12.2(5th)SB on the Cisco uBR10012 Universal Broadband Router to support software upgrades without service interruption on supported, redundantly-configured cable line cards. The RLC ISSU process is the second phase of ISSU support in the ISSU-uBR10K feature and is supported only on the Cisco uBR10-MC5X20S/U/H cable line cards on the Cisco uBR10012 router. The dual TCC+ or DTCC+ cards are sequentially reloaded after running the issu runversion command.

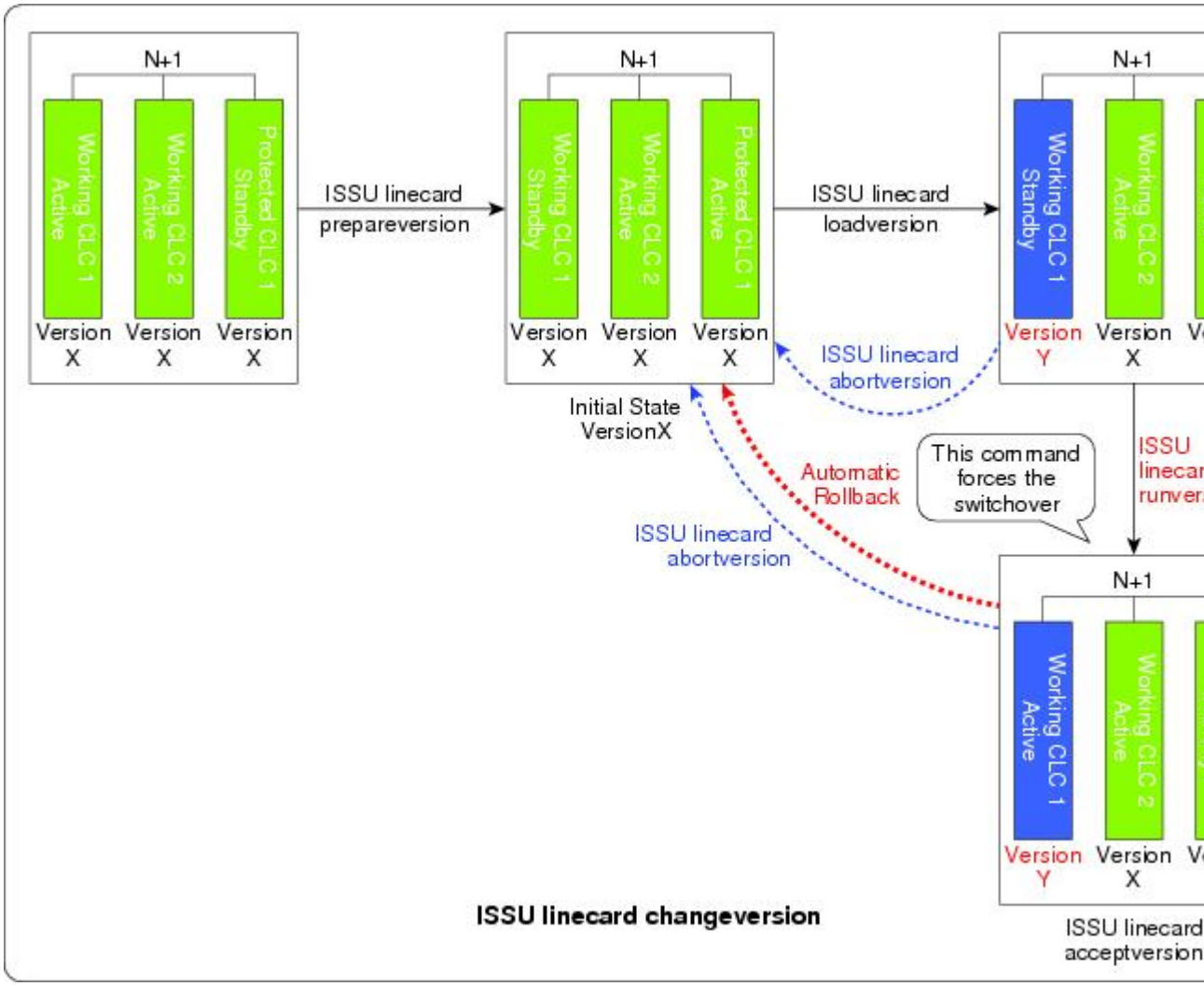
The RLC ISSU process has some dependencies with the RP ISSU process. First, the RLC ISSU process can be started only when the RP ISSU process reaches the Run Version (RV) state. In the RV state, the RP rollback timer is stopped (via the **issu acceptversion** command) and the active RP is running the new version of the software image. Each of the cable line cards have reconnected to the new RP and ISSU image negotiation has occurred between the RP and the cable line cards (See Figure below).

Figure 17: RP ISSU Process Stages With WAN Line Card MDR



At this point in the RP ISSU process, the stages of the RLC ISSU process can be executed. The stages of the RLC ISSU process are comparable to the stages that occur in the RP ISSU process. The RLC ISSU process itself can be initiated to run manually or automatically. In the manual method, the Prepare Version (only in RLC ISSU process), Load Version, Run Version, and Accept Version stages are executed in step-by-step fashion by running the corresponding **issu linecard** command for each stage of the process. In the automatic method, a single command (**issu linecard changeversion**) is executed to run each of these stages back-to-back and automatically as each stage completes (Figure below).

Figure 18: RLC ISSU Process Stages

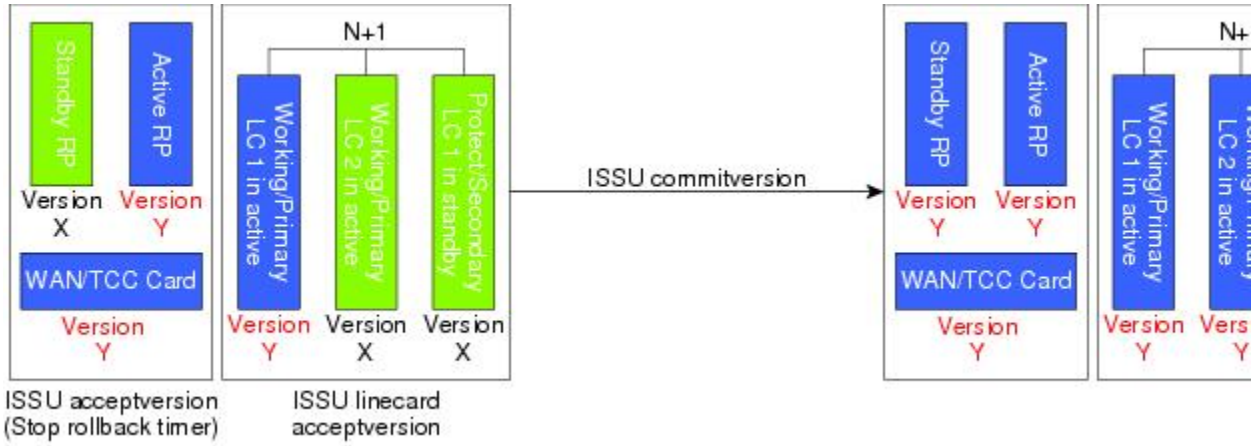


The RLC ISSU process runs serially for each targeted cable line card. A subsequent cable line card may start the process when the previous cable line card's RLC ISSU process is complete. This process is different from the ISSU process for other line cards supporting MDR, which reloads simultaneously during the Run Version stage of the RP ISSU process.

Finally, when the RLC ISSU process is complete for all redundant cable line cards, a condition is set such that the RP ISSU Commit Version stage can be executed. The RP and RLC ISSU processes share the Commit

Version stage such that the **issu commitversion** command confirms both the RP and RLC images at the same time (Figure below).

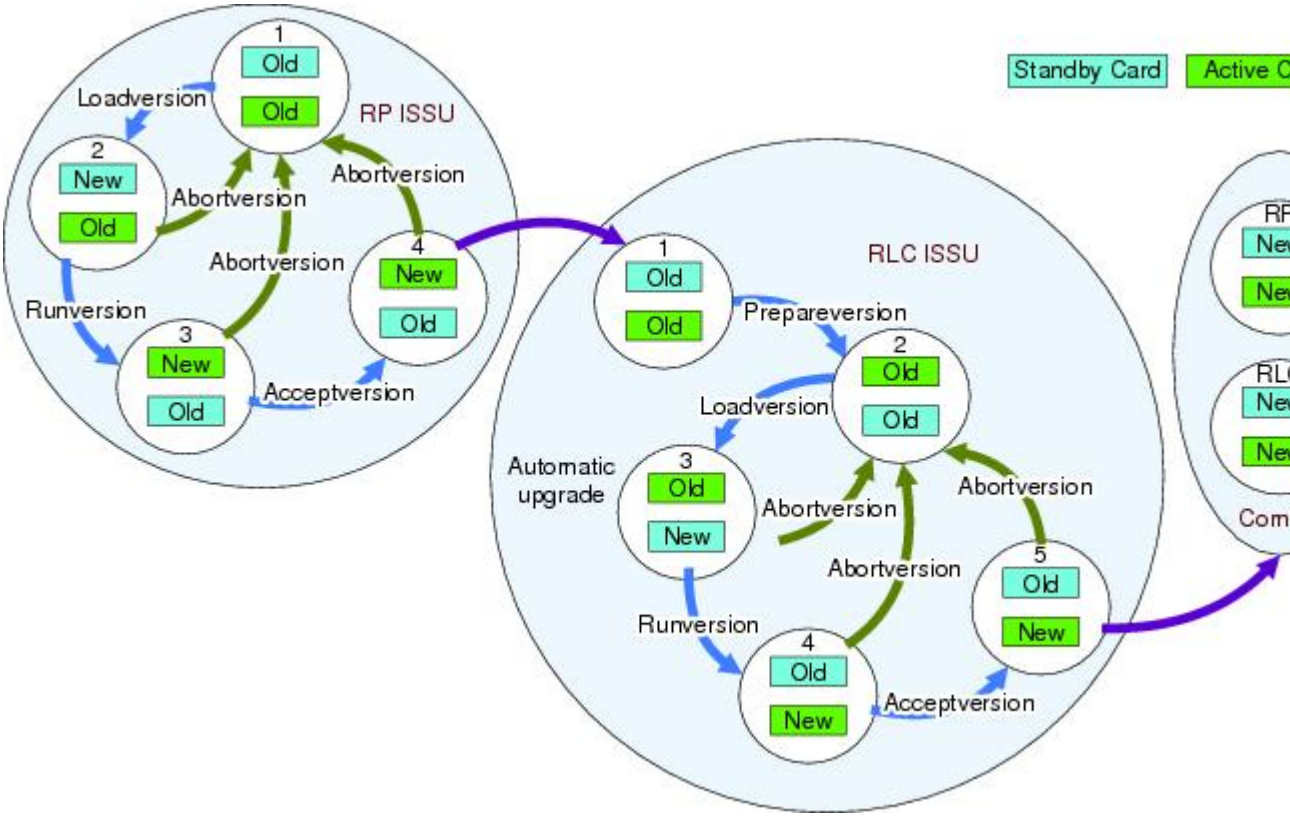
Figure 19: Combined RP and RLC ISSU Commit Version Stage



While the RLC ISSU process also supports the functions of aborting a version upgrade as the RP ISSU process does, it has the additional functions of stopping an automatic RLC ISSU process, stopping other RLC ISSU processes in the middle of execution, and reloading a version. The Reload Version function is intended to support cable line cards that are not configured for redundancy and that do not support the MDR function of the RP ISSU process.

Figure below provides a graphical overview of these RP and RLC ISSU processes.

Figure 20: RP and RLC ISSU Process Summary View



Versioning Capability in Cisco IOS Software to Support ISSU

Before the introduction of the ISSU capability, the SSO mode of operation required each RP to be running like versions of Cisco IOS software. The operating mode of the system in a redundant HA configuration is determined by exchanging version strings when the standby RP registers with the active RP.

The system entered SSO mode only if the versions running on the both RPs were the same. If not, the redundancy mode was reduced to ensure compatibility. With ISSU capability, the implementation allows two different but compatible release levels of Cisco IOS images to interoperate in SSO mode and enables software upgrades while packet forwarding continues. Version checking done before ISSU capability was introduced is no longer sufficient to allow the system to determine the operating mode.

ISSU requires additional information to determine compatibility between software versions. Therefore, a compatibility matrix is defined that contains information about other images with respect to the one in question. This compatibility matrix represents the compatibility of two software versions, one running on the active and the other on the standby RP, and to allow the system to determine the highest operating mode it can achieve. Incompatible versions will not be able to progress to SSO operational mode.

The Cisco IOS infrastructure has been internally modified and redesigned to accommodate subsystem versioning with ISSU. Cisco IOS subsystems correspond to feature sets and software component groupings. Features or subsystems that maintain state information across RPs are HA-aware or SSO clients. A mechanism called ISSU Framework, or ISSU protocol, allows subsystems within Cisco IOS software to communicate RP to RP

and to negotiate the message version for communication between RPs. Internally, all NSF- and SSO-compliant applications or subsystems that are HA-aware must follow this protocol to establish communication with their peer across different versions of software. (For further information on operating modes, see the Stateful Switchover document.)

Compatibility Matrix

You can perform the ISSU process when the Cisco IOS software on both the active and the standby RP is capable of ISSU and the old and new images are compatible. The compatibility matrix information stores the compatibility among releases as follows:

- Compatible—The base-level system infrastructure and all optional HA-aware subsystems are compatible. An in-service upgrade or downgrade between these versions will succeed with minimal service impact. The matrix entry designates the images to be compatible (C).
- Base-level compatible—One or more of the optional HA-aware subsystems is not compatible. An in-service upgrade or downgrade between these versions will succeed; however, some subsystems will not be able to maintain state during the transition. The matrix entry designates the images to be base-level compatible (B).
- Incompatible—A core set of system infrastructure exists that must be able to interoperate in a stateful manner for SSO to function correctly. If any of these required features or protocols is not interoperable, then the two versions of the Cisco IOS software images are declared to be incompatible. An in-service upgrade or downgrade between these versions is not possible. The matrix entry designates the images to be incompatible (I).

The compatibility matrix represents the compatibility relationship a Cisco IOS software image has with all of the other Cisco IOS software versions within the designated support window (for example, all of those software versions the image "knows" about) and is populated and released with every image. The matrix stores compatibility information between its own release and prior releases. It is always the newest release that contains the latest information about compatibility with existing releases in the field. The compatibility matrix is available within the Cisco IOS software image and on Cisco.com so that users can determine in advance whether an upgrade can be done using the ISSU process.

Before attempting an ISSU, you should determine the compatibility level between the Cisco IOS software versions on the active and the standby RPs. To display the compatibility matrix data between two software versions on a given system, enter the show issu comp-matrix negotiated command.

Compatibility Information for ISSU-uBR10K on the Cisco uBR10012 Universal Broadband Router

The **show issu comp-matrix negotiated** command provides information about the compatibility for the Cisco IOS software images on the active and standby PRE-2 cards. Compatibility information between the RP images and LC images, or LC to LC images is not explicitly reported in this output.

However, if the **show issu comp-matrix negotiated** command indicates compatibility between RP images, then RP to LC, and LC to LC image compatibility is also supported.

The following example shows sample output from the **show issu comp-matrix negotiated** command on the Cisco uBR10012 Universal Broadband Router:

```
Router# show issu comp-matrix negotiated
CardType: uBR10000(107), Uid: 2,  Image Ver: 12.2(20070219:204203)145
Image Name: UBR10K2-K9P6U2-M

Cid     Eid     Sid     pSid    pUid      Compatibility
=======================================================
2       1       65538   65542   15        COMPATIBLE
```

```
2       1       65543   65542   11      COMPATIBLE
2       1       65549   65543   17      COMPATIBLE
2       1       65579   4       1       COMPATIBLE
3       1       65577   6       1       COMPATIBLE
4       1       65567   13      1       COMPATIBLE
5       1       65547   27      1       COMPATIBLE
7       1       65570   5       1       COMPATIBLE
8       1       65572   11      1       COMPATIBLE
9       1       65540   0       2       COMPATIBLE
9       1       65541   0       2       COMPATIBLE
9       1       65545   0       2       COMPATIBLE
9       1       65563   0       2       COMPATIBLE
9       1       65569   2       1       COMPATIBLE
9       1       65573   0       2       COMPATIBLE
9       1       65575   0       2       COMPATIBLE
10      1       60      0       2       COMPATIBLE
```

ISSU-Capable Protocols and Applications

The following protocols and applications support ISSU:

- ISSU - ARP —ARP supports ISSU.
- ISSU - ATM—The ATM application supports ISSU. The application requirements for ISSU are as follows:
  - Identify the ATM client as nonbase
  - Support message versioning of ATM HA event synchronous messages
  - Provide capability exchange between peers
- ISSU - Dynamic Host Configuration Protocol (DHCP) on-demand address pool (ODAP) client/server—This feature supports ISSU.
- ISSU - DHCP proxy client—The DHCP proxy client feature supports ISSU.
- ISSU - DHCP relay on unnumbered interface—The DHCP relay on unnumbered interface feature supports ISSU.
- ISSU - DHCP server—The DHCP server feature supports ISSU.
- ISSU - DHCP snooping—DHCP snooping supports ISSU.
- ISSU - EtherChannel - PagP LACP—PagP and LACP support ISSU.
- Cisco Express Forwarding—Cisco Express Forwarding (CEF) supports ISSU.
- ISSU - FHRP/GLBP—The Gateway Load Balancing Protocol (GLBP) supports ISSU.
- ISSU - FHRP/HSRP—The Hot Standby Router Protocol (HSRP) supports ISSU.
- ISSU - Frame Relay—The Frame Relay protocol supports ISSU.
- ISSU - HDLC—The High-Level Data Link Control (HDLC) protocol supports ISSU.
- ISSU - IEEE 802.1x—The IEEE 802.1x protocol supports ISSU.
- ISSU - IEEE 802.3af—IEEE 802.3af supports ISSU.
- ISSU - IGMP snooping—IGMP snooping supports ISSU.
- ISSU - IP Host—The IP host supports ISSU.

- ISSU - IS-IS - IS-IS protocol supports ISSU.
- ISSU - MPLS L3VPN—Multiprotocol Label Switching (MPLS) supports ISSU. For information about upgrading ISSU MPLS-related applications through ISSU, see the *ISSU MPLS Clients* document.
- ISSU - Port Security—Port security supports ISSU.
- ISSU - PPP/MLP—The PPP and multilink PPP (MLP) protocols support ISSU.
- ISSU - QoS support—The Quality of Service (QoS) feature supports ISSU.
- ISSU - Remote File System—The Remote File System (RFS) versioning feature supports ISSU.
- ISSU - SNMP—SNMP supports ISSU.
- ISSU - STP—STP supports ISSU

Restrictions for ISSU-Capable Protocols and Applications With ISSU-uBR10K

The following protocols and applications are not supported with ISSU-uBR10K:

- ISSU - ATM
- ISSU - FHRP/GLBP
- ISSU - FHRP/HSRP
- ISSU - Frame Relay
- ISSU - HDLC
- ISSU - IEEE 802.1x
- ISSU - IEEE 802.3af
- ISSU - IGMP snooping
- ISSU - Port Security
- ISSU - PPP/MLP
- ISSU - STP

SNMP Support for ISSU

ISSU - SNMP for SSO provides a mechanism for synchronizing the SNMP configurations and the MIBs that support SSO from the active RP to the standby RP, assuming that both RPs are running the same version of Cisco IOS software. This assumption is not valid for ISSU.

ISSU - SNMP provides an SNMP client that can handle ISSU transformations for the MIBs. An SNMP client (SIC) handles ISSU for all MIBs and handles the transmit and receive functions required for ISSU. During SNMP, a MIB is completely synchronized from the active RP to the standby RP only if the versions of the MIB on both Cisco IOS releases are the same.

MDR Support for ISSU

Minimum Disruptive Restart (MDR) is a feature that allows line cards to be restarted to minimize the disruption of traffic passing through the system. It prevents line protocol flaps and minimizes traffic disruption across

a restart or reload of software. The uBR10K platform supports MDR of the Cisco 10000-SIP-600 jacket card and the SPA-24XDS-SFP (Wideband DOCSIS SPA). ISSU prevents network outage whenever the 10000-SIP-600 card or the Wideband SPA card reloads.

The advantages of the MDR feature in ISSU are:

- Reduces the time for a line card to pass data traffic after the card's reload.
- Maintains data and configuration during the software restart or reload.
- Retains the status of the line card after MDR.

Note MDR supports only minor changes in software, while the line cards reload in case of a major change in software or firmware.

MDR and FPGA Upgrade

Most often when performing MDR ISSU upgrade for the Cisco 10000-SIP-600 jacket card and the SPA-24XDS-SFP, only the firmware is upgraded - the FPGA will remain intact. However, there might be some rare cases where the FPGA will need to be upgraded. In these cases, the MDR ISSU process will become FPGA upgrade process. Unlike MDR ISSU, FPGA Upgrade will cause all traffic passing through the Cisco 10000-SIP-600 jacket card to be completely disrupted. During this FPGA upgrade process, the new FPGA will be downloaded to each SPA. It takes approximately 12 minutes to download the new FPGA to each SPA.

The FPGA upgrade process is an independent process from the system ISSU process. The system ISSU process triggers the FPGA upgrade process during the issu runversion step, and will continue to upgrade other cable line cards in the system. These two processes execute at the same time, and one process can finish before the other.

The show upgrade fpd progress command can be used to check the status of the FPGA upgrade process.

ISSU Single-Step Upgrade Process

Single-step upgrade process is the ability of the ISSU feature to upgrade the entire CMTS system using the **issu changeversion** command. This process allows the corresponding networking device to inform the system that the networking device is performing a complete upgrade cycle automatically, and the state transitions to move to the next step automatically.

The ISSU upgrade process consists of three states:

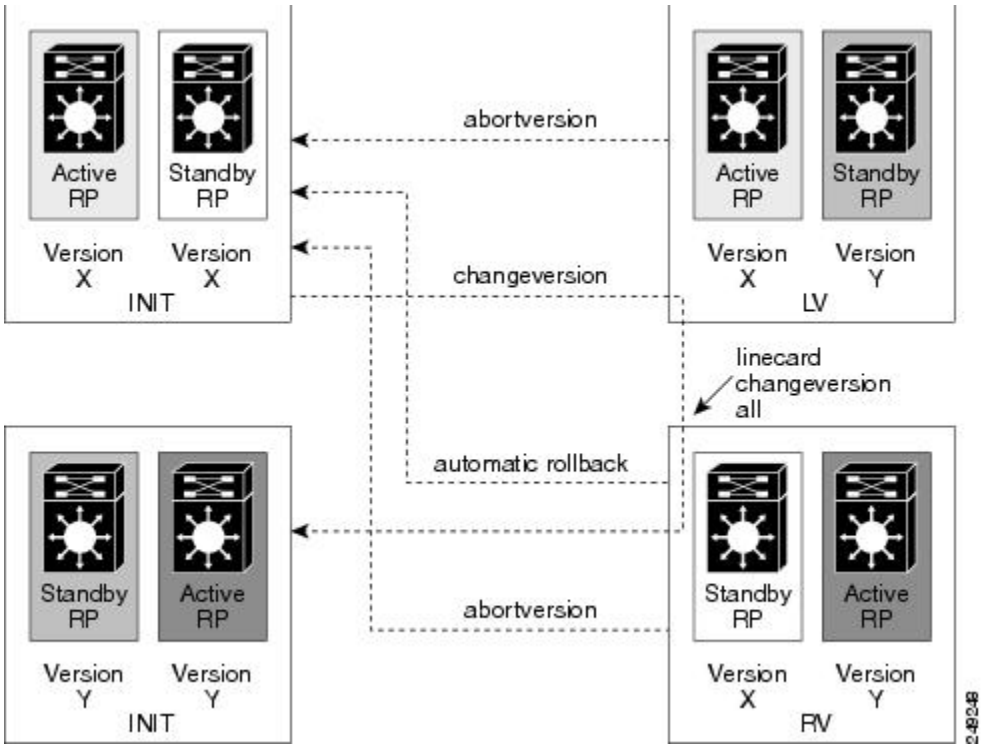
1. Initialization (INIT) state—It is the steady state before any software upgrade is committed.
2. Load version (LV) state—It is the state when the issu loadversion command is executed to start the ISSU process.
3. Run version (RV) state—It is the state when the issu runversion command is executed to force a switchover from the active Route Processor (RP) to the standby RP.

Each of these states is defined by a set of variables, that is, primary version (PV), secondary version (SV), current version (CV), and ISSU state (IS). The transition of all these states is accomplished using the **issu changeversion** command, which automatically performs these state transitions.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU can be performed using the single step upgrade process using the **issu changeversion** command.

Figure below provides a graphical overview of the single-step upgrade process.

Figure 21: Single-step Upgrade Process Summary View



The advantages of the Single-Step Upgrade process are:

- Reduces human interaction during the ISSU upgrade cycle.
- Avoids executing multiple commands to complete the ISSU cycle.

How to Perform the RP ISSU Process

Unlike SSO, which is a mode of operation for the device and a prerequisite for performing RP ISSU, the ISSU process is a series of steps performed while the router or switch is in operation. The steps result in the implementation of new or modified Cisco IOS software, and have a minimal impact to traffic.

Restrictions for Performing the RP ISSU Process

The following list provides basic restrictions for performing the RP ISSU process:

- Even with ISSU, it is recommended that upgrades be performed during a maintenance window.

- The new features should not be enabled (if they require change of configuration) during the ISSU process.
- In a downgrade scenario, if any feature is not available in the downgrade revision Cisco IOS software image, that feature should be disabled prior to initiating the ISSU process.

Restrictions for Performing the RP ISSU Process on the Cisco uBR10012 Universal Broadband Router

- The RP ISSU process is supported beginning in Cisco IOS Release 12.2(33)SCB using the following Cisco IOS software images:
  - ubr10k2-k9p6u2-mz
  - ubr10k4-k9p6u2-mz
- The RP ISSU process is supported beginning in Cisco IOS Release 12.2(5th)SB using the following Cisco IOS software image:
  - ubr10k2-k9p6u2-mz
- If you are performing the RP and RLC ISSU process on the Cisco uBR10012 Universal Broadband Router, read first the How to Perform the Redundant LC ISSU Process, on page 775. This section describes which RP ISSU tasks are prerequisites for the RLC ISSU process.

Note The examples provided in the RP ISSU process sections of this document reflect certain Cisco 10000 Series Router software image names. Be aware when referring to these examples that you replace these sample image names with the appropriate supported image name for your platform.

The tasks in the following sections explain how to complete the ISSU process:

Restrictions for Performing the RP-only ISSU Process on the Cisco uBR10012 Universal Broadband Router

Effective from Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU process is supported using the following Cisco IOS line card software images:

– ubr10kg4clc-lck8-mz

ISSU Multi-Step Upgrade Process

The ISSU multi-step upgrade process consists of the following tasks:

Note Starting Cisco IOS Release 12.2(33)SCD2 onwards, you can you can complete the RP upgrade using the ISSU Single-Step Upgrade Process, on page 772 and skip the tasks mentioned above.

Note Effective from Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process may be performed using the three steps of the ISSU Multi-Step Upgrade Process or the t_ISSU_Single-Step_Upgrade_Process_1150348.xml#task_1150348.

Loading Cisco IOS Software on the Standby RP

This task describes how to use ISSU to load a new Cisco IOS software to the standby RP.

Before You Begin

- Ensure that both the active and the standby RPs are configured in SSO mode. Refer to the *Stateful Switchover* document for more details on how to configure SSO mode on RPs.
- Ensure that the new version of Cisco IOS software image is already loaded in the file system of both the active and standby RPs. Also ensure that appropriate boot parameters are set for the standby RP.
- Optionally, customers may want to perform additional tests and commands to determine the current state of peers and interfaces for later comparison.
- Ensure that there is console access to both PREs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**issu loadversion***active-slot active-image**standby-slot standby-image* [**force** **Example:** `Router# issu loadversion a disk0:ubr10k2-k9p6u2-mz.new b stby-disk0:ubr10k2-k9p6u2-mz.new`	Starts the ISSU process. It may take several minutes after the **issu loadversion** command is entered for Cisco IOS software to load onto the standby RP and for the standby RP to transition to SSO mode.
Step 3	**show issu state** [**detail** **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process. At this point in the ISSU process, use this command to check that the standby RP is loaded and is in SSO mode. It may take several seconds after entering the **issu loadversion** command for Cisco IOS software to load onto the standby RP and the standby RP to transition to SSO mode. If you enter the **show issu state** command too soon, you may not see the information you need.

Switching to the Standby RP

This task describes how to switch to the standby RP, which is running the new Cisco IOS software image.

Note Run the show redundancy states command to view the current redundancy status and make sure the system has reached SSO before executing the issu runversion command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**issu runversion active-slot-name [active-image-URL]** **Example:** `Router# issu runversion b stby-disk0:ubr10k2-k9p6u2-mz.new`	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image. The image URL is optional.

Stopping the RP ISSU Rollback Timer

The following task describes how to stop the rollback timer. If the rollback timer is not stopped, the system automatically aborts the RP ISSU process and reverts to the original Cisco IOS software version if the next RP ISSU procedure is not performed prior to the rollback timer timeout. For example, the RP ISSU process would abort after the **issu acceptversion** command was entered only if the **issu runversion** command was not entered before rollback timeout.

Note Once you successfully stop the RP ISSU rollback timer using the **issu acceptversion** command, you can begin to execute the RLC ISSU process as applicable for redundant cable line cards on the Cisco uBR10012 Universal Broadband Router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**issu acceptversion***active-slot-name* [*active-image-URL*] **Example:** `Router# issu acceptversion b disk0:ubr10k2-k9p6u2-mz.new`	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process. The image URL is optional.

Verifying the RP ISSU Software Installation

During the RP ISSU process, there are three valid states: init, load version, and run version. Use the show issu state command to get information on each or all of these states:

- Init state—The initial state is two RPs, one active and one standby, before the ISSU process is started.
- Load version (LV) state—The standby RP is loaded with the new version of Cisco IOS software.
- Run version (RV) state—The issu runversion command forces the switchover of the RPs. The newly active RP now runs the new Cisco IOS software image.

You can verify the ISSU software installation by entering **show** commands that provide information on the state of theduring the ISSU process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show issu state** [**A** | **B** | **detail** **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process.
Step 3	**show redundancy**[**clients** | **config-sync** | **counters** | **force-rpr** | **history** | **idb-sync-history** | **interlink** | **linecard** | **platform** | **states** | **switchover**] **Example:** `Router# show redundancy`	Displays the current or historical status, mode, and related redundancy information about the device.

ISSU Single-Step Upgrade Process

You can upgrade the entire CMTS system by issuing the issu changeversion command. This command executes individual ISSU phases in the correct sequence automatically, and reduces the human effort involved in executing the other ISSU commands. The issu changeversion command upgrades the router processors first and then upgrades the line cards.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade may be deployed using the Single-Step Upgrade Process by issuing the **issu changeversion** command.

When the issu changeversion command is issued, it executes the functionality of the issu loadversion, issu runversion, issu acceptversion, issu linecard changeversion all and issu commitversion commands, without any user intervention required to navigate through each step of the single-step upgrade process.

The single-step upgrade process involves the following steps:

1. Run the issu changeversion command. This command invokes the issu loadversion command to reload the standby RP with the new Cisco IOS image.
2. The reload triggers the issu runversion command to switch over the RP from Active to Standby state to run the new Cisco IOS image.
3. After the two RPs reach the Stateful Switchover (SSO) mode, the single-step upgrade process resumes on the newly active RP with the new image to complete individual line card upgrades using the line card changeversion all command.
4. The single-step upgrade process on the active RP executes the issu commitversion command to complete the entire upgrade.

Note The issu changeversion command also upgrades the line card ISSU process. This command executes the linecard changeversion command before the issu commitverison command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu changeversion** *image to upgrade* **Example:** `Router# issu changeversion disk0:ubr10k4-k9p6u2-mz.122-33.SCC2`	Upgrades the CMTS system for a specific Cisco IOS image.

Aborting a Software Upgrade Using ISSU

You can abort the ISSU process at any stage manually by issuing the issu abortversion command. The ISSU process also aborts on its own if the software detects a failure.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process may be aborted by using the **issu abortversion** command.

Note Always abort the active RP in conjunction with the target Cisco IOS release.

If you abort the process after you issue the issu loadversion command, then the standby RP is reset and reloaded with the original software.

If the process is aborted after either the **issu runversion** or **issu acceptversion** command is entered, then a second switchover is performed to the new standby RP that is still running the original software version. The RP that had been running the new software is reset and reloaded with the original software version.

This task describes how to abort the ISSU process before a user has committed to the process by issuing the **issu commitversion** command.

Beginning Cisco IOS Release 12.2(5th)SB, if the RP ISSU process is aborted on the Cisco uBR10012 universal broadband router using the **issu abortversion** command, or the RP is rolled back due to a switchover, the **issu linecard abortversion** command must also be executed. For more information, see the Manually Rolling Back a Software Upgrade Using RLC ISSU, on page 783.

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu abortversion** *slot image* **Example:** `Router# issu abortversion b disk0:ubr10k2-k9p6u2-mz.new`	Cancels the ISSU upgrade or downgrade process that is in progress and restores the router to its state before the process had started.

Configuring the Rollback Timer to Safeguard Against Upgrades

The Cisco IOS software maintains an ISSU rollback timer. The rollback timer provides a safeguard against an upgrade that may leave the new active RP in a state in which communication with the RP is severed.

A user may want to configure the rollback timer to fewer than 45 minutes (the default) so that the user need not wait in case the new software is not committed or the connection to the router was lost while it was in runversion mode. A user may want to configure the rollback timer to more than 45 minutes in order to have enough time to verify the operation of the new Cisco IOS software before committing the new image.

Once you are satisfied that the ISSU process has been successful and you want to remain in the current state, you must indicate acceptance by issuing the **issu acceptversion** command, which stops the rollback timer. Therefore, entering the **issu acceptversion** command is extremely important to moving the ISSU process forward.

Issuing the **issu commitversion** command at this stage is equal to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for a period of time and are satisfied with the new software version.

This task explains how to configure the rollback timer.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**configure issu set rollback timer** *seconds* **Example:** `Router(config)# configure issu set rollback timer 3600`	Configures the rollback timer value.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns the user to privileged EXEC mode.
Step 5	**show issu rollback timer** **Example:** `Router# show issu rollback timer`	Displays the current setting of the ISSU rollback timer.

Displaying ISSU Compatibility Matrix Information

The ISSU compatibility matrix contains information about other software images about the version in question. This compatibility matrix represents the compatibility of the two software versions, one running on the active and the other on the standby RP, and the matrix allows the system to determine the highest operating mode it can achieve. This information helps the user identify whether or not to use ISSU.

This task explains how to display information about the ISSU compatibility matrix.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu comp-matrix** {**negotiated** | **stored** **Example:** `Router# show issu comp-matrix`	Displays information regarding the ISSU compatibility matrix.

How to Perform the Redundant LC ISSU Process

Just as with RP ISSU, the RLC ISSU process is a series of steps performed while the router is in operation. The steps result in the implementation of a new or modified software image on a cable line card, and have minimal impact to traffic. The RLC ISSU process can be run automatically for certain cable line cards or globally for all cable line cards, or you can run the process manually for individual cable line cards.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the Redundant LC ISSU Process is optional while performing the RP-only ISSU Upgrade process. The Redundant LC ISSU Process need not be performed if the new image used for the upgrade is an RP-only ISSU Upgrade image.

Prerequisites for Performing the Redundant LC ISSU Process

- For the ISSU process to run on cable line cards, the cable line cards must be configured for N+1 redundancy.

For more information about configuring N+1 redundancy, refer to the “N+1 Redundancy for the Cisco Cable Modem Termination System” chapter of the Cisco CMTS Feature Guide at:

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

Note For cable line cards that are not configured redundantly, you can manually load images using the **issu linecard reloadversion** command. However, this type of upgrade cannot be executed without affecting the network availability of the cable line card. For more information about how to do this, see the Reloading Non-Redundant Cable Line Cards, on page 784.

- Be sure that the following software image prerequisites are met:
  - The old and new versions of the RP and LC software images must be ISSU-capable and compatible. The LC software image is bundled with the RP image. For more information about software image compatibility for RLC ISSU, see the Compatibility Information for ISSU-uBR10K on the Cisco uBR10012 Universal Broadband Router, on page 763.
  - Both the original and target line card images need to be downloaded to disk or bootflash areas, but not necessarily on the same device. Because the image size is greater than 32MB, two images might not fit on a single flash device. You can put either image on disk0, disk1, or bootflash.
  - Verify that the system is configured to automatically boot the new image using the following global configuration command:

```
Router(config)# config-register 0x2
```

- Verify that the **boot system** global configuration command is configured for the path that specifies the location of the new target image, as shown in the following example:

```
Router(config)# boot system disk0:ubr10k2-k9p6u2-mz.new
```

- The following tasks must be run before the RLC ISSU process can begin:
  - Loading Cisco IOS Software on the Standby RP, on page 769 (required)
  - Switching to the Standby RP, on page 769 (required)
  - Stopping the RP ISSU Rollback Timer, on page 770 (required)
  - Verifying the RP ISSU Software Installation , on page 771 (required)

Once you verify that the active RP is in Run Version (RV state) after using the **issu acceptversion** command, you can begin the RLC ISSU process.

Restrictions for Performing the Redundant LC ISSU Process

The following list describes the restrictions for performing the RLC ISSU process:

- As with RP ISSU, it is recommended that upgrades be performed during a maintenance window.
- Any new features should not be enabled (if they require a change of configuration) during the RLC ISSU process.
- In a downgrade scenario, if any feature is not available in the downgrade revision of the line card software image, that feature should be disabled prior to initiating the RLC ISSU process.

- Do not run the **issu commitversion** command before performing the RLC ISSU process. The RLC ISSU process can not be executed if the RP is in the INIT state.
- N+1 fault protection is not disabled while the RLC ISSU process is in progress. However, the secondary (or protect) cable line card will not be available to provide redundancy services for a failing primary (or working) cable line card while the protect cable line card has become active for another working line card during the RLC ISSU process. Once the activated protect cable line card goes back to its standby state, it will again be available for redundant failover.

If a working line card fails during this period while the protect line card is unavailable, the working line card will reload with the software image that corresponds to the currently active RP. N+1 synchronization between the working and protect line cards is maintained.

- You cannot configure any line card redundancy commands or initiate any line card switchovers while an automatic or manual RLC ISSU process is in progress.
- The RLC ISSU process is not SSO capable. Therefore, the RLC ISSU process needs to be restarted on a newly active RP.
- Partial upgrades between RP and LC versions is not supported. Therefore, the RP and each LC should be upgraded to the same version. When you commit the new version using the **issu commitversion** command, both the RP and LC images are confirmed and enabled in the new standby RP card and protected cable line card.
- The RLC ISSU process does not support any configurable rollback timers. However, there are certain platform-dependent timeout values associated with the various stages of the RLC ISSU process within which the different stages are expected to complete. These timeout values apply to both the automated and manual execution of the RLC ISSU process. If a stage of the RLC ISSU process does not complete within the timeout period, an error results. An error message is produced and the RLC ISSU process is stopped.

The timeout values for the Cisco uBR10012 router are:

-
  - Waiting for line cards to prepare for switchover—240 seconds. This timer begins when either **issu linecard prepareversion** or **issu linecard changeversion** commands are issued.
  - Switchover timer—240 seconds. This timer runs as part of the **issu linecard prepareversion** or **issu linecard changeversion** command to allow completion of the line card switchover.
  - **issu linecard loadversion** command—360 seconds. Time allowed for the Load Version stage to complete.
  - **issu linecard runversion** command—240 seconds. Time allowed for the Run Version stage to complete.
  - **issu linecard reloadversion** command—360 seconds. Time allowed for the Reload Version stage to complete.

The tasks in the following sections explain how to perform the RLC ISSU process:

- Use one of the following required methods to run the RLC ISSU process:
  - Running the RLC ISSU Process Automatically, on page 778 or
  - Running the RLC ISSU Process Manually, on page 779

- Verifying the RLC ISSU Software Installation, on page 781 (required)
- Forcing the RLC ISSU Process to Run , on page 783 (optional)
- Manually Rolling Back a Software Upgrade Using RLC ISSU, on page 783 (optional)
- Reloading Non-Redundant Cable Line Cards, on page 784 (optional)
- Finishing the ISSU Process to Enable the New Cisco IOS Software Version on the RP and Cable Line Cards, on page 785 (required)

Running the RLC ISSU Process Automatically

When you run the RLC ISSU process automatically using the **issu linecard changeversion** command, you can specify running the process for all redundant cable line cards, or for specified working cable line cards.

If you want to force the RLC ISSU process regardless of the image version status, or you want to ignore any potential service outage and error handling, use the **issu linecard changeversion forced** form of the command.

You can also use the **issu linecard changeversion** command to restart the RLC ISSU process if you previously used the **issu linecard process stop** command.

Note If you include any non-redundant cable line cards as part of the automatic RLC ISSU process, please run the **issu linecard reloadversion** command for the non-redundant line card. For more information, see the Reloading Non-Redundant Cable Line Cards, on page 784.

Once the automatic RLC ISSU process is complete, you need to verify the installation and commit the RP and LC images. The following sections describe these tasks:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard changeversion all** | *slot_1 /subslot_1*]. . .[*slot_n/subslot_n*]} [**forced** **Example:** `Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1`	Starts the ISSU process to run all stages automatically for the specified cable line cards. **Note** It is preferred to use the all *option.*

Stopping the Automatic RLC ISSU Process

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

You can stop the automatic RLC ISSU process if you want to interrupt the process from continuing for the next cable line card that is configured for RLC ISSU.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard process stop** **Example:** `Router# issu linecard process stop`	Stops the automatic RLC ISSU process from continuing for the next specified cable line card.

Running the RLC ISSU Process Manually

The tasks in the following sections explain how to perform the RLC ISSU process manually:

Once you accept the RLC ISSU process, you can begin the manual RLC ISSU process for another cable line card. If you have completed the RLC ISSU process, then you need to verify the installation and commit the RP and LC images. The following sections describe these tasks:

The following sections explain optional tasks that you can perform as part of the manual RLC ISSU process:

Manually Switching the Primary Working Cable Line Card to Standby

To begin the RLC ISSU process manually, use the **issu linecard prepareversion** command and specify the slot/subslot location of the primary working cable line card. When you enter this command, the redundant configuration and image version of the cable line card are checked. If the image version needs to be changed, then a switchover occurs placing the primary working cable line card in standby mode, and activating the protect cable line card.

If you want to force the switchover regardless of the image version status, or you want to ignore any potential service outage and error handling, use the **issu linecard prepareversion forced** form of the command.

You can also use the **issu linecard prepareversion** command to restart the RLC ISSU process if you previously used the **issu linecard process stop** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard prepareversion** *slot*/*subslot* [**forced** **Example:** `Router# issu linecard prepareversion 6/0`	Manually starts the ISSU process for the specified working cable line card. During this stage the working cable line card switches to standby, and the protect cable line card becomes active.

Manually Loading the New Image on the Primary Line Card in Standby

To load the new target line card image on the specified working cable line card that is currently in standby mode as part of the manual RLC ISSU process, use the **issu linecard loadversion** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard loadversion** *slot* / *subslot* **Example:** `Router# issu linecard loadversion 6/0`	Loads the new target line card image on the specified working cable line card.
Step 3	**show hccp brief** **Example:** `Router# show hccp brief`	Displays summary information about the N+1 line card redundancy configuration.

Manually Switching to the Standby Cable Line Card

To initiate an N+1 switchover to the current standby cable line card (the original working primary cable line card) as part of the manual RLC ISSU process, use the **issu linecard runversion** command. During this stage, the primary working cable line card becomes active (with the new target image) for all of the interfaces on

the secondary protect cable line card. A 3-second rollback timer for the primary working cable line card is started.

If you want to force the switchover regardless of any image version incompatibility, or you want to ignore any potential service outage and error handling, use the **issu linecard runversion forced** form of the command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard runversion** *slot* /*subslot* [**forced**] **Example:** `Router# issu linecard runversion 6/0`	Starts a switchover to the current standby cable line card.

Accepting the RLC ISSU Process

To mark completion of and accept the Prepare Version, Load Version, and Run Version stages of the RLC ISSU process, use the **issu linecard acceptversion** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard acceptversion** *slot* / *subslot* **Example:** `Router# issu linecard acceptversion 6/0`	Stops the RLC ISSU rollback timer.

Verifying the RLC ISSU Software Installation

During the RLC ISSU process, there are many different valid states. Use the show issu linecard state command display these line card states:

- PSLC READY state—Waiting for the protect (or secondary) line card to become ready for line card switchover.
- PREPAREVERSION state—Waiting for the line card switchover from working (primary) to protect (secondary) to complete.
- LOADVERSION state—Waiting for the original working/primary line card to finish loading the new image, and become standby-ready for the secondary line card.
- RUNVERSION state—Waiting for completion of the line card switchover to reactivate the original working/primary line card with the new image.
- ACCEPTVERSION state—Transient state for performing Accept Version stage of process.
- RELOAD state—Completed manual execution of the **issu linecard reloadversion** command.
- SINGLE OP PV DONE state—Completed manual execution of the **issu linecard prepareversion** command.
- SINGLE OP LV DONE state—Completed manual execution of the **issu linecard loadversion** command.
- SINGLE OP RV DONE state—Completed manual execution of the **issu linecard runversion** command.

You can also use some other **show** commands to display the status of the N+1 redundancy configuration and the status of the RP ISSU process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu state**[slot / port] [**detail**] **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process.
Step 3	**show issu linecard state** | **history** **Example:** `Router# show issu state`	Displays the state of theduring the RLC ISSU process.
Step 4	**show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **states** | **inter-device**] **Example:** `Router# show redundancy`	Displays current or historical status, mode, and related redundancy information about the device.

	Command or Action	Purpose
Step 5	**show hccp brief** **Example:** `Router# show hccp brief`	Displays summary information about the N+1 line card redundancy configuration.

Forcing the RLC ISSU Process to Run

You can configure the automatic RLC ISSU process, or certain stages of the manual RLC ISSU process to continue processing regardless of any potential service outage and subsequent error handling, by using the **forced** keyword option on the corresponding commands.

For more information, see the following topics:

Manually Rolling Back a Software Upgrade Using RLC ISSU

If you determine that the system running the new software image does not function as expected, you can configure the RLC ISSU process to roll back all cable line cards or certain cable line cards to the previous version using the **issu linecard abortversion** command.

If you want to force the abort process and ignore any potential service outage and error handling, use the **issu linecard abortversion forced** form of the command.

Note If the RP ISSU process is aborted using the **issu abortversion** command, or the RP is rolled back due to a switchover, the **issu linecard abortversion** command must also be used.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard abortversion** {**all** | *slot*/*subslot*} [**forced**] **Example:** `Router# issu linecard abortversion 6/0`	Cancels the RLC ISSU operation and reloads the cable line card with the original version of the line card image prior to the RLC ISSU process.

Reloading Non-Redundant Cable Line Cards

To load a new target line card image on a cable line card that is not configured redundantly, use the **issu linecard reloadversion** command.

Caution While executing, the **issu linecard reloadversion** command will disrupt network services for the specified non-redundant cable line card.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard reloadversion** {*original-image* | *target-image*} {**all** | *slot_1*[/*subslot_1*]. . .[*slot_n*[/*subslot_n*] **Example:** `Router# issu linecard reloadversion disk0:ubr10k2-k9p6u2-mz.new 6/0`	Loads the new target line card image on the specified working cable line card.

Stopping a Manual RLC ISSU Process

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

To manually stop any RLC ISSU operation, use the **issu linecard process stop** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**issu linecard process stop** **Example:** `Router# issu linecard process stop`	Stops the current RLC ISSU operation.

Restarting a Stopped RLC ISSU Process

If you have previously stopped an RLC ISSU operation using the **issu linecard process stop** command, you can restart the process using either the **issu linecard changeversion** or **issu linecard prepareversion** commands.

The RLC ISSU process will restart at the next logical ISSU operation to be performed depending on the current state of the system.

For more information about how to use these commands, see the Running the RLC ISSU Process Automatically, on page 778 or the Manually Switching the Primary Working Cable Line Card to Standby, on page 779.

Finishing the ISSU Process to Enable the New Cisco IOS Software Version on the RP and Cable Line Cards

After loading new Cisco IOS software to the standby RP, causing the standby RP to become the active RP and the former active RP to become the standby RP, you need to enable the new standby RP to use the new Cisco IOS software version. This task explains how to perform that process.

Beginning in Cisco IOS Release 12.2(5th)SB on the Cisco uBR10012 Universal Broadband Router, the **issu commitversion** command is used to confirm both the new RP and new LC images that were upgraded using the RLC ISSU process.

Note The **issu commitversion** command can be executed only when all of the primary cable line cards are upgraded to the latest target image, either by **issu linecard changeversion** command, or **issu linecard reloadversion** command or by system reset.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the **issu commitversion** command is must be used for completing the RP-only ISSU Upgrade process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**issu commitversion standby-slot-name** [**standby-image-url**] **Example:** `Router# issu commitversion a stby-disk0:ubr10k2-k9p6u2-mz.new`	Allows the new Cisco IOS software image to be loaded into the standby RP.

Configuration Examples for Performing ISSU

This section contains the following configuration examples:

Note The examples provided in the RP ISSU process sections of this document reflect certain Cisco 10000 Series Router software image names. Be aware when referring to these examples that you must replace these sample image names with the appropriate supported image name for your platform.

Example: Verifying Redundancy Mode Before Beginning the ISSU Process

Before you begin the ISSU process, verify the redundancy mode for the system. NSF and SSO must be configured before attempting an ISSU. The following example displays verification that the system is in SSO mode and that slot A—RP A is the active R, and slot B—RP B is the standby RP. Both RPs are running the same Cisco IOS software image.

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 0

Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
Redundancy State              = SSO
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 45
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
Router# show redundancy
Redundant System Information :
```

```
------------------------------
       Available system uptime = 18 minutes
Switchovers system experienced = 0
             Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up
Current Processor Information :
------------------------------
               Active Location = slot A
        Current Software state = ACTIVE
       Uptime in current state = 17 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower
NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                          BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                   CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2

Peer Processor Information :
----------------------------
              Standby Location = slot B
        Current Software state = STANDBY HOT
       Uptime in current state = 16 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower
NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                          BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                   CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
```

Example: Verifying the ISSU State

The following example provides information about the ISSU state:

```
Router# show issu state detail

                          Slot = A
                    RP State = Active
                   ISSU State = Init
                  Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
                 Variable Store = PrstVbl
                          Slot = B
                    RP State = Standby
                   ISSU State = Init
                  Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
Slot Red Role  Peer Act/Sby  Image Match RP LC ISSU State      ISSU Proc
---- --------- ---- -------- -------------- ------------------ ----------
5/0  Secondary -    standby  Yes            -                  -
6/0  Primary   5/0  active   Yes            -                  -
7/0  Primary   5/0  active   Yes            -                  -
8/0  Primary   5/0  active   Yes            -                  -
```

```
PRE is the new active: FALSE
Waiting for MDR:  FALSE
No Transitional Line Card State information registered.
No Peer Line Card State information registered.
Peer Line Card Action:
-------Card Type-------- -----Action------ --Slots---
24rfchannel-spa-1        NO ACTION         0x00000004
4jacket-1                NO ACTION         0x00000004
2cable-dtcc              NO ACTION         0x00000028
1gigethernet-hh-1        NO ACTION         0x00000200
```

The new version of the Cisco IOS software must be present on both of the RPs. The initial bootflash directory examples show the presence of the old image, and the disk0 directory information shows that the new version is present on both disks.

```
Directory of bootflash:/

    1  -rw-     2530312   Jan 1 2000 01:42:10 +00:00  c10k2-eboot-mz.122-16.BX
    2  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.old

Directory of stby-bootflash:/

    1  -rw-     2530312   Jan 1 2000 01:42:10 +00:00  c10k2-eboot-mz.122-16.BX
    2  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.old

Directory of disk0:/

    1  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.new

Directory of stby-disk0:/

    1  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.new
```

Examples for Performing the RP ISSU Process

The following examples explain how to verify the ISSU software installation by entering **show** commands that provide information on the state of the RPs during the ISSU process.

Example: Initiating the RP ISSU Process

To initiate the ISSU process, enter the issu loadversion command as shown in the following example:

```
Router# issu loadversion a disk0:ubr10k2-k9p6u2-mz.new b stby-disk0:ubr10k2-k9p6u2-mz.new
```

The following two examples display the ISSU state and redundancy state after ISSU process initiation:

```
Router# show issu state
                         Slot = A
                    RP State = Active
                   ISSU State = Load Version
               Boot Variable = bootflash:ubr10k2-k9p6u2-mz.old,12;
                         Slot = B
                    RP State = Standby
                   ISSU State = Load Version
               Boot Variable =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
Router# show redundancy state
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 0
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
     Split Mode = Disabled
   Manual Swact = Enabled
```

```
 Communications = Up
   client count = 31
client_notification_TMR = 30000 milliseconds
          RF debug mask = 0x0
```

Example: Forcing a Switchover from the Active RP to the Standby RP

At this point, the system is ready to switch over and run the new version of Cisco IOS software that has been loaded onto the standby RP. When you enter the issu runversion command, an SSO switchover will be performed, and NSF procedures will be invoked if so configured.

```
Router# issu runversion b stby-disk0:ubr10k2-k9p6u2-mz.new
```

Once the ISSU process has been completed, the system will be running the new version of software and the previously active RP will now become the standby RP. The standby will be reset and reloaded, but it will remain on the previous version of software and come back online in STANDBY-HOT status. The following example shows how to connect to the newly active RP and verify these conditions.

```
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 24 minutes
Switchovers system experienced = 1
              Standby failures = 0
        Last switchover reason = user initiated
                 Hardware Mode = Duplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up
Current Processor Information :
-------------------------------
               Active Location = slot B
        Current Software state = ACTIVE
       Uptime in current state = 8 minutes
            Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M), Version
 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                         BOOT =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
Peer Processor Information :
----------------------------
              Standby Location = slot A
        Current Software state = STANDBY HOT
       Uptime in current state = 6 minutes
            Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M), Version
 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                        BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
Router# show issu state
                           Slot = B
                      RP State = Active
                     ISSU State = Run Version
                  Boot Variable =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
                           Slot = A
                      RP State = Standby
                     ISSU State = Run Version
                  Boot Variable = bootflash:ubr10k2-k9p6u2-mz.old,12;
```

The new active RP is now running the new version of software, and the standby RP is running the old version of software and is in the STANDBY-HOT state.

Example: Stopping the RP Rollback Process

In the following example, the "Automatic Rollback Time" information indicates the amount of time left before an automatic rollback will occur. Enter the issu acceptversion command within the time period specified by the rollback timer to acknowledge that the RP has achieved connectivity to the outside world; otherwise, the ISSU process is terminated, and the system reverts to the previous version of Cisco IOS software by switching to the standby RP.

```
Router# show issu rollback-timer

Rollback Process State = In progress
Configured Rollback Time = 45:00
Automatic Rollback Time = 29:03
```

Entering the issu acceptversion command stops the rollback timer:

```
Router# issu acceptversion b disk0:
ubr10k2-k9p6u2-mz.new
```

Example: Committing the New Software to the Standby RP

The following example shows how to commit the new Cisco IOS software image in the file system of the standby RP and ensure that both the active and the standby RPs are in the run version (RV) state. The standby RP is reset and reloaded with the new Cisco IOS software and returned to STANDBY-HOT status.

```
Router# issu commitversion a stby-disk0:
ubr10k2-k9p6u2-mz.new
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Secondary
        Unit ID = 1
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 31
 client_notification_TMR = 30000 milliseconds
          RF debug mask = 0x0
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 35 minutes
Switchovers system experienced = 1
              Standby failures = 1
        Last switchover reason = user initiated
                  Hardware Mode = Duplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up
Current Processor Information :
-------------------------------
               Active Location = slot B
        Current Software state = ACTIVE
       Uptime in current state = 18 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.CISCO070530) NIGHTLY BUILD, synced to V122_32_8_23_SBK
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

```
Compiled Tue 30-May-07 02:02 by torowe
                      BOOT = disk0:ubr10k2-k9p6u2-mz.new,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
Peer Processor Information :
----------------------------
              Standby Location = slot A
        Current Software state = STANDBY HOT
       Uptime in current state = 4 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.CISCO070530) NIGHTLY BUILD, synced to V122_32_8_23_SBK
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 30-May-07 02:02 by torowe
                      BOOT = disk0:ubr10k2-k9p6u2-mz.new,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
Router# show issu state
                           Slot = B
                     RP State = Active
                    ISSU State = Init
               Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

                           Slot = A
                     RP State = Standby
                    ISSU State = Init
               Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;
Router# show issu state detail
                           Slot = B
                     RP State = Active
                    ISSU State = Init
               Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k2-k9p6u2-mz.new
                           Slot = A
                     RP State = Standby
                    ISSU State = Init
               Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k2-k9p6u2-mz.new
```

The ISSU process has been completed. At this stage, any further Cisco IOS software version upgrade or downgrade will require that a new ISSU process be invoked.

Example: Aborting the RP ISSU Process

The following example shows how to abort the RP ISSU process manually:

```
Router# issu abortversion b disk0:ubr10k2-k9p6u2-mz.new
```

If you abort the process after you have entered the **issu loadversion** command, then the standby RP is reset and is reloaded with the original software version.

Example: Verifying RP Rollback Timer Information

To display rollback timer information for the RP ISSU process, enter the **show issu rollback-timer** command:

```
Router# show issu rollback-timer
        Rollback Process State = In progress
```

```
      Configured Rollback Time = 45:00
       Automatic Rollback Time = 29:03
```

Example: Verifying the ISSU Single Step Upgrade

The following example provides information about the state and current version of the RPs including the Single Step Upgrade process.

```
Router# show issu state detail

                        Slot = A
                   RP State = Active
                  ISSU State = Init
                Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
               Operating Mode = SSO
             Primary Version = N/A
           Secondary Version = N/A
             Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
              Variable Store = PrstVbl
                        Slot = B
                   RP State = Standby
                  ISSU State = Init
                Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
               Operating Mode = SSO
             Primary Version = N/A
           Secondary Version = N/A
             Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
Slot Red Role  Peer Act/Sby  Image Match RP LC ISSU State      ISSU Proc
---- --------- ---- -------- -------------- ------------------ ---------
5/0  Secondary -    standby  Yes            -                  -
6/0  Primary   5/0  active   Yes            -                  -
7/0  Primary   5/0  active   Yes            -                  -
8/0  Primary   5/0  active   Yes            -                  -
PRE is the new active: FALSE
Waiting for MDR:  FALSE
No Transitional Line Card State information registered.
No Peer Line Card State information registered.
Peer Line Card Action:
-------Card Type-------- -----Action------ --Slots---
24rfchannel-spa-1        NO ACTION         0x00000004
4jacket-1                NO ACTION         0x00000004
2cable-dtcc              NO ACTION         0x00000028
1gigethernet-hh-1        NO ACTION         0x00000200
```

Configuration Examples for Performing RLC ISSU

This section provides configuration examples for the RLC ISSU process. It includes the following sections:

Configuration Examples for the Automatic RLC ISSU Process

This section provides the following configuration examples:

Example: Initiating the RLC ISSU Process for all Cable Line Cards

The following example shows how to initiate the RLC ISSU process automatically for all cable line cards in a redundant configuration:

```
Router> enable
Router# issu linecard changeversion all
```

Example: Initiating the RLC ISSU Process for Specific Cable Line Cards

The following example shows how to initiate the RLC ISSU process automatically for certain working cable line cards in a redundant configuration:

```
Router> enable
Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1
```

Example: Stopping the Automatic RLC ISSU Process

The following example shows how to stop the automatic RLC ISSU process in between the ISSU process for each configured cable line card:

```
Router# issu linecard changeversion stop
```

Example: Forcing an Automatic RLC ISSU Process

The following example shows how to force the automatic RLC ISSU process and ignore any error processing:

```
Router> enable
Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1 forced
```

or, alternatively:

```
Router> enable
Router# issu linecard changeversion all forced
```

Configuration Examples for the Manual RLC Process

Example: Performing the RLC ISSU Process Manually

The following example shows how to run the complete RLC ISSU process manually for a specified working cable line card installed in slot 6 and subslot 0 of the Cisco uBR10012 router:

```
Router> enable
Router# issu linecard prepareversion 6/0
Router# issu linecard loadversion 6/0
Router# issu linecard runversion 6/0
Router# issu linecard acceptversion 6/0
Router# issu commitversion a disk0:ubr10k2-k9p6u2-mz.new
```

Example: Manually Rolling Back a Software Upgrade Using RLC ISSU

The following example shows how to manually roll back the line card software image to the original version:

```
Router# issu linecard abortversion 6/0
```

Example: Reloading Non-Redundant Cable Line Cards

The following example shows how to load a software image for a specific cable line card that is not configured redundantly:

```
Router# issu linecard reloadversion disk0:ubr10k2-k9p6u2-mz.new 6/0
```

Example: Stopping a Manual RLC ISSU Process

The following example shows how to stop any manual RLC ISSU operation:

```
Router# issu linecard process stop
```

Additional References

The following sections provide references related to performing ISSU.

Related Documents

Related Topic	Document Title
Performing ISSU	*Cisco IOS Software: Guide to Performing In-Service Software Upgrades*
Information about Cisco Nonstop Forwarding	*Cisco Nonstop Forwarding* http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnsf20s.html
Information about stateful switchover	*Stateful Switchover* http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html
ISSU and MPLS clients	ISSU MPLS Clients
Information about N+1 line card redundancy	"N+1 Redundancy for the Cisco Cable Modem Termination System" chapter of the Cisco CMTS Feature Guide http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISSU

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

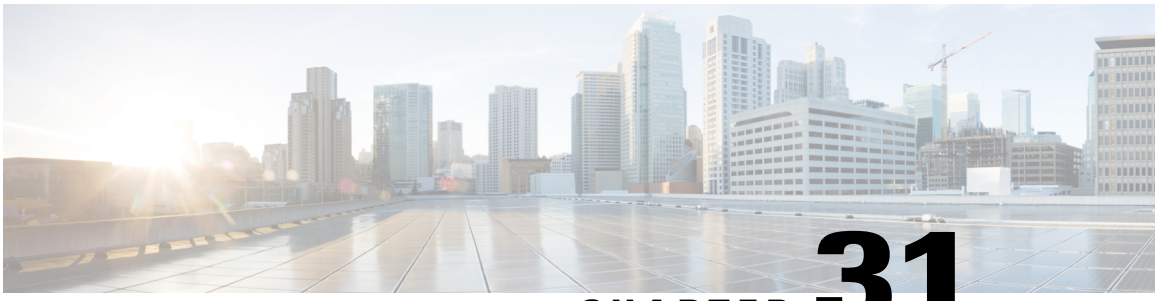
Table 86: Feature Information for ISSU

Feature Name	Releases	Feature Information
	12.2(5th)SB	Support for the ISSU-uBR10K feature was introduced on the Cisco uBR10012 Universal Broadband Router with the Performance Routing Engine 2.
	12.2(31)SB2	Support for the following new features were added to the 12.2(31)SB2 release: • ISSU - Dynamic Host Configuration Protocol (DHCP) on-demand address pool (ODAP) client/server • ISSU - DHCP proxy client • ISSU - DHCP relay on unnumbered interface • ISSU - DHCP server • ISSU - First Hop Routing Protocol (FHRP) - Gateway Load Balancing Protocol (GLBP) • ISSU - Intermediate System-to-Intermediate System (IS-IS) • ISSU - Quality of Service (QoS)

Feature Name	Releases	Feature Information
	12.2(31)SGA	Support for ISSU was introduced on the Cisco Catalyst 4500 series platform. Support for the following new features was added on the Cisco Catalyst 4500 series platform: • Dynamic Host Configuration Protocol (DHCP) snooping • EtherChannel - Port Aggregation Protocol (PagP) and Link Aggregate Control Protocol (LACP) • IEEE 802.1x protocol • IEEE 802.3 • Internet Group Management Protocol (IGMP) snooping • IP Host • Port security • Spanning-Tree Protocol (STP) The following commands were introduced or modified: **configure issu set rollback timer**, **issu abortversion**, **issu acceptversion**, **issu commitversion**, **issu load version**, **issu runversion**, **show issu comp-matrix**, **show issu state**.
	12.2(28)SB	This feature was introduced.

Feature Name	Releases	Feature Information
ISSU	12.2(33)SCB	Support for the following new features were added to this release. • ISSU Compatibility Matrix • Minimal Disruptive Restart (MDR) and the Cisco Wideband SPA • Cable ISSU Clients • Support for Performance Routing Engine 4 • Support for 10000-SIP-600 (4-bay Cisco 10000 SPA jacket card) • Support for Wideband SPA • ISSU Time Enhancement The following commands were introduced or modified: **issu linecard abortversion**, **issu linecard acceptversion**, **issu linecard changeversion**, **issu linecard loadversion**, **issu linecard prepareversion**, **issu linecard reloadversion**, **issu linecard runversion**.
ISSU	12.2(33)SCB3	A general prerequisite for Cisco uBR10012 router was added. The following commands were introduced or modified: **show processes cpu**, **show controllers cable [proc-cpu]**.
Single Step Upgrade Process	12.2(33)SCD2	This feature was introduced on the Cisco CMTS routers to perform a single-step complete ISSU upgrade process cycle using the new issu changeversion command.
ISSU	12.2(33)SCG	Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

Feature Name	Releases	Feature Information
RP-only ISSU Upgrade	12.2(33)SCH2	Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process supports the upgrade of only the RP images without upgrading the line card images.



CHAPTER 31

N+1 Redundancy for the Cisco Cable Modem Termination System

First Published: February 14, 2008

Last Updated: October 01, 2012

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The N+1 Redundancy feature provides high availability on CMTS and telecommunications networks that use broadband media. 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. The N+1 redundancy protection scheme you select for your system depends on your CMTS platform and upon the number of cable interface line cards or broadband processing engines (BPEs) that you have installed in the Cisco CMTS router.

Note This document describes the N+1 redundancy configuration and support with the Cisco uBR 3x10 RF Switch in detail. Starting with Cisco IOS Release 12.2(33)SCG, support for the Cisco uBR Advanced RF Switch has been added. For the N+1 redundancy configuration and support information with the Cisco uBR Advanced RF Switch, see the Cisco uBR Advanced RF Switch Software Configuration Guide .

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites

To use N+1 redundancy, ensure the following conditions are met:

- To implement N+1 redundancy, you must use an image from a supported Cisco IOS software release. Refer to the release notes for your platform on Cisco.com to verify the availability of the N+1 Redundancy feature.
- Your downstream plant must meet Data-over-Cable Service Interface Specifications (DOCSIS 1.0 or later) requirements.
- Customer cable modems must meet requirements for your network and server offerings. All third-party cable modems must comply with DOCSIS 1.0 or later versions.

Table below shows the hardware compatibility prerequisites for the N+1 Redundancy feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 87: N+1 Redundancy Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [54]

54 The Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Note Cisco uBR7200 series routers do not support N+1 redundancy.

Restrictions and Limitations

The following sections describe restrictions and guidelines for configuring N+1 line card redundancy.

Note It is important to be aware that in Cisco IOS software releases earlier to Cisco IOS Release 12.2(33)SCC, line card redundancy is configured in two ways: N+1 HCCP Redundancy and Global N+1 Line Card Redundancy. The N+1 HCCP Redundancy configuration is not supported beginning with Cisco IOS Release 12.2(33)SCC. As you consider the restrictions and configuration information in this chapter, keep the distinction between the legacy HCCP configuration and the global configuration in mind.

General N+1 Redundancy Restrictions

The following are the general restrictions applicable to the N+1 Redundancy feature. These restrictions apply to both N+1 HCCP Redundancy and Global N+1 Line Card Redundancy configurations.

- A DOCSIS Timing, Communication and Control (DTCC) card or a TCC+ card must be installed in your Cisco uBR10012 router in order to employ the Cisco RF Switch in your cable headend system. For more detailed information on the DTCC and TCC+ cards, see the following documents:
  - Cisco uBR10012 Universal Broadband Router DTCC Card
  - Cisco uBR10012 Universal Broadband Router TCC+ Card

- Using slot 5/1 as the protect interface is easiest for physical wiring to the Cisco RF Switch when used with the Cisco uBR10012 router.
- The Cisco uBR10012 SNMP community string and N+1 Cisco RF Switch community string must be different. If the same community string is used, the Cisco uBR10012 router cannot be reached through SNMP until the community string is adjusted.
- The HCCP Switchover Enhancements feature has the following restrictions:
  - The feature is supported on the Cisco uBR10012 router only.
  - The line card switchover performance improvements are valid for networks scaling to less than 5000 cable modems per line card, and less than 1000 voice calls per line card.
  - The working and protect line cards must have the same channel width.
  - Upconverter failure detection is not included as part of the line card switchover performance improvements.
  - Virtual interface bundling is required. If you are upgrading from an earlier Cisco IOS software release and virtual bundling is not configured upon startup, the Cisco IOS software will automatically generate a virtual bundling configuration. Therefore, beginning in Cisco IOS Release 12.3(21)BC, Layer 3 information cannot be configured directly at the cable interface. The maximum number of virtual bundle interfaces supported is 40, and bundle numbers can be between 1–255.
  - In Cisco IOS Release 12.2(33)SCA and later, keepalive failure detection is enabled only for upstreams that have 15 or greater modems online. However, a switchover due to keepalive failure will trigger only if there is not any traffic on all of the upstreams associated with a cable interface that is enabled for keepalive.

For example, on a cable line card interface enabled for keepalive (this is the default) you have the following US status: US0 (200 CMs online), US1 (10 CMs online), US2 (16 CMs online), US3 (shutdown). US0 and US2 are enabled for keepalive detection because they each have more than 15 modems online.

If US0 has a keepalive failure due to a cable cut, but US2 is still passing traffic, then no keepalive switchover is triggered on that domain or interface. The calculation looks at all relevant US ports in a MAC domain and if those relevant ports have no traffic, then keepalive detection will begin. In this example, only two ports were relevant and both of those ports did not lose traffic, so keepalive still did not activate the failover.

If US0 had a cable cut while US2 also had no traffic, then a keepalive switchover would be triggered.

Note Beginning with Cisco IOS Release 12.2(33)SCE and later, the High Availability keepalive failure detection feature is disabled on Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards to prevent false alarms. The downstream connectivity loss can be detected by DEPI control session on the Cisco uBR-MC3GX60V line card whereas downstream PHY is able to detect the fatal error on the Cisco UBR-MC20X20V line card.

Information About N+1 Redundancy

This section describes the concepts that relate to N+1 redundancy: N+1 redundancy refers to (N) cable interface line cards, called “working” line cards being protected by one additional line card (+1), called the “protect” line card.

The two types of Cisco N+1 configuration are as follows:

- 7+1—Refers to an eight-card redundancy scheme in which seven working cable interface line cards are protected by one additional protect line card. This is the default N+1 configuration for the Cisco uBR10012 router, and requires two Cisco uBR 3x10 RF Switches or one Cisco uBR Advanced RF Switch.

Note The term "7+1 Redundancy" is also referred to as "8+1 Redundancy" in the field—physically, eight line cards in "8+1" mode are configured as seven working line cards with one protect line card. Therefore, "7+1 Redundancy" is the more physically accurate term.

- 4+1—Refers to a four-card redundancy scheme in which four working cable interface line cards are protected by one additional protect line card. This requires only one Cisco RF Switch.

Upconverters may reside between the Cisco uBR 3x10 RF Switch and the downstream (DS) interface on the Cisco CMTS. Cisco IOS supports both SNMP and non-SNMP-capable upconverters. No upconverters are required with the Cisco uBR Advanced RF Switch.

Note Globally configured N+1 line card redundancy and the legacy form of HCCP line card redundancy configurations are mutually exclusive in Cisco IOS Release 12.2(33)SCB and earlier.

You can configure N+1 redundancy in the following two ways:

N+1 HCCP Redundancy

Configured using HCCP commands at the interface level.

N+1 redundancy adds synchronization between Hot-Standby Connection-to-Connection Protocol (HCCP) working interface configurations and those inherited upon switchover to HCCP protect interfaces. This makes the configuration of both easier and switchover times faster.

Note N+1 HCCP Redundancy configuration is supported only in Cisco IOS Release 12.2(33)SCB and earlier.

Restrictions for N+1 HCCP Redundancy

Use the IP address from the local loopback interface (required in SCA and SCB only) as the working interface IP address when configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router. We recommend that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface IP address to the HCCP protect configuration.

Restrictions with the Cisco UBR10-MC 5X20 Cable Interface Line Card

- MAC domains and corresponding DS interface pairs switch over together— Each ASIC processor on the Cisco UBR10-MC 5X20 line card supports two MAC domains. MAC domains that share a common ASIC processor (JIB) must be configured so that they share the same state, Active or Standby. As a result, each interface in the pair switches over with the other.

Downstream MAC domain pairings would be downstream (DS) ports 0 and 1, ports 2 and 3, and a solitary port 4, which has its own JIB. For example, these interface pairings share the same JIB and switch over together as follows:

- ◦ Cable interface 5/0/0 and 5/0/1
  ◦ Cable interface 5/0/2 and 5/0/3
  ◦ Cable interface 5/0/4 is on the third ASIC processor, which is not shared with another interface.
- If Cisco uBR10-MC5X20 line card is used as working line card and Cisco uBR-MC20X20V line card used as protect line card, the HCCP feature is not supported when the working line card is replaced (using Online Insertion and Removal (OIR)) with a Cisco uBR-MC20X20V line card.

Note If HCCP is not configured on an interface that shares a MAC processor with another configured interface, it does not switch over and could cause issues. The same holds true if an ASIC companion is "locked out" during a failover.

Prerequisites for N+1 HCCP Redundancy

Before a switchover can occur, the HCCP protect interface automatically loads multiple configurations from the HCCP working interface. All configurations are loaded to protect automatically except DS modulation, DS interleave depth, and the DOCSIS Annex mode. If protect interface configuration occurs at the time of switchover, the PHY parameters are reset and cable modems go offline. To prevent this scenario, the protect interface is synchronized with the latest 'sync' status received from any working interface. Therefore, it is required that all HCCP working interfaces within an HCCP group have identical configurations for the command-line interfaces described in this section. Any one of these working interfaces provides the configuration of HCCP protect interfaces.

Preconfiguring HCCP Protect Interfaces

The following three specific HCCP functions are synchronized between working and protect interfaces:

- downstream modulation—the modulation scheme used for downstream traffic to the subscriber's cable modem.
- downstream interleave depth—the interleaving amount of downstream symbols for impulse noise issues
- the DOCSIS Annex mode—the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card:
  ◦ Annex A (Europe)
  ◦ Annex B (North America)

Each of these three preconfigurations should be the same for all members of the HCCP groups; otherwise the cable modem may go offline during switchover and the switchover performance may be impacted due to the delay in applying the new change in the downstream PHY chip.

Global N+1 Line Card Redundancy

Global N+1 Line Card Redundancy feature simplifies the configuration of working and protect interfaces by eliminating the need to configure the more complex **hccp** interface configuration commands. Global N+1 Line Card Redundancy is supported on the Cisco uBR10012 router only.

The following set of simpler CLIs are used to configure global N+1 line card redundancy:

- **redundancy** command in global configuration mode
- **linecard-group cable** command in redundancy configuration mode. This command auto-enables line card redundancy configuration mode.
- **member subslot** command in line card redundancy configuration mode

Note The **member subslot** commands implement HCCP on each cable interface for the line card subslot position.

This feature allows plug-and-play operation of the Cisco RF switch in 7+1 HCCP Redundancy configuration with the Cisco uBR10012 universal broadband router because the Cisco RF switch is shipped with certain default settings to allow a quick bringup of a 7+1 redundant configuration with the router. However, some configuration of the router is required.

Global 4+1 Redundancy on the Cisco uBR10012 Router

This configuration entails one Cisco RF Switch and the router. In this configuration, four working interfaces are supported with one protect interface, but at a line card level. When one interface on a line card switches over, this triggers switchover for the entire line card.

Global 7+1 Redundancy on the Cisco uBR10012 Router

This configuration entails two Cisco uBR 3x10 RF Switches or one Cisco uBR Advanced RF Switch and the router. In this configuration, seven working interfaces are supported with one protect interface, but at a line card level. When one interface on a line card switches over, this triggers switchover for the entire line card.

Cisco IOS and Cisco RF Switch Firmware for N+1 Redundancy

Two operating systems govern the configuration and operation of N+1 redundancy on the Cisco CMTS:

- Cisco Internetwork Operating System (IOS)—Governs the configuration and operation of Cisco universal broadband routers, and works closely with Cisco RF Switch when configured in N+1 redundancy.

Note The Cisco IOS CLI synchronizes configurations between HCCP working and protect interfaces. Preconfiguration of the protect interfaces is no longer required in most circumstances.

- Cisco uBR 3x10 RF Switch Firmware—Governs the configuration and operation of the Cisco RF Switch, including the IP address on the RF Switch.

Refer to the Cisco RF Switch Firmware Command Reference Guide on Cisco.com for complete feature descriptions and command histories for the Firmware Versions listed above.

Note With the Cisco uBR 3x10 RF Switch, both command-line interfaces are required for configuration and testing of N+1 redundancy.

- Cisco uBR Advanced RF Switch—The Cisco uBR10012 router controls the configuration and operation of the Cisco uBR Advanced RF Switch.

Refer to the Cisco uBR Advanced RF Switch Software Configuration Guide and Cisco IOS CMTS Cable Command Reference for complete feature descriptions and command usage.

N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router

The 7+1 redundancy scheme for the Cisco uBR10012 router supports redundancy for the cable interface line cards installed in a fully populated Cisco uBR10012 chassis. Other redundancy schemes are designed to support partial cable interface line card populations in a Cisco uBR10012 chassis.

A single Cisco uBR10012 CMTS can support up to eight Cisco cable interface line cards.

A single Cisco RF Switch can then be connected to this Cisco uBR10012 router, allowing you to deploy an N+1 redundancy scheme where one protecting cable interface line card supports from one to seven working cable interface line cards in the same chassis.

N+1 Redundancy and the Cisco RF Switches

The Cisco RF Switch can be operated in two separate modes, either in 7+1 configuration, or in 4+1 configuration.

Note The default N+1 redundancy mode for the Cisco RF Switch is 7+1. This does not require change when configuring N+1 redundancy on the Cisco uBR10012 router.

Note The show configuration command and other Cisco RF Switch commands contain the Card Protect Mode field. When this field displays 7+1, this indicates that the Cisco RF Switch is configured for N+1 redundancy, where eight or less working line cards are possible.

In both of the Cisco RF Switches, the slot number is the chassis slot in which an Ethernet controller or an upstream or downstream card is installed, and the logical interface number is the physical location of the interface port on an Ethernet controller.

The Cisco RF switch module is a switching matrix that allows flexibility in the routing of RF signals between "N" working RF cable interface line cards and one protect RF cable interface line card.

IF Muting on the Cisco CMTS for non-SNMP-Capable Upconverters

IF muting with both SNMP and non-SNMP-capable upconverters is supported in 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 routers.

- IF Muting offers the additional benefit of being faster than RF Muting.
- IF Muting is enabled by default.

IF Muting functions in the following manner:

- IF output from the working cable interface line card is enabled.
- IF output from the protect cable interface line card is disabled.
- When a switchover occurs from working to protect, the IF output of the working card is disabled and that of the protect is enabled. If an interface is in Active mode, RF output is enabled.
- When the cable interface line card first comes up after a system failure, IF output is muted until the Cisco CMTS determines if each interface is in active or standby mode (in either working or protect state). When an interface is active (working or protect), IF output is enabled. When an interface is in standby mode, IF output is muted.

The relevance and support for IF Muting is dependent on the type of Cisco CMTS being used. This is a summary of IF Muting in relation to three sample scenarios:

- Case1—External upconverters are not controlled nor controllable. In this type of scenario, the external upconverter either cannot be controlled remotely or the Cisco CMTS is not configured to control the external upconverter.
- Case 2—The Cisco CMTS is configured to control an external upconverter. Cisco continues to support N+1 redundancy in this scenario (in which IF Muting is not required). The Cisco CMTS uses RF Muting of the upconverter in this scenario—automatically enabled when an HCCP upconverter statement is configured.
- Case 3—The Cisco CMTS uses internal upconverter(s). Cisco continues to support N+1 redundancy in this scenario (in which IF muting is not required). The Cisco CMTS uses RF muting in this scenario (automatically enabled) because the upconverter is configured by the CMTS to do RF Muting.

IF Muting and HCCP Configuration

HCCP interface configuration typically entails three tasks:

- Working or protect mode
- Upconverter statement
- RF switch statement

When you configure HCCP on an interface, but you do not specify an upconverter statement, this dictates whether IF Muting is active. With no upconverter statement in the interface configuration, IF Muting becomes active by default.

Restrictions for IF Muting

Shared Downstream Frequency

All the interfaces in the same HCCP group must use the same downstream frequency. To define the downstream center frequency for the cable interface line card, use the cable downstream frequency command in cable

interface configuration mode. On cable interfaces with an integrated upconverter, use the no form of this command to remove the downstream frequency and to disable the RF output.

The usable center frequency range depends on whether the downstream is configured for DOCSIS or EuroDOCSIS operations:

- ◦ DOCSIS — 91 to 857 MHz
  ◦ EuroDOCSIS — 112 to 858 MHz

The Cisco IOS supports a superset of these standards, and setting a center frequency to a value outside these limits violates the DOCSIS or EuroDOCSIS standards. Cisco does not guarantee the conformance of the downstream and upconverter outputs when using frequencies outside the DOCSIS or EuroDOCSIS standards.

Requirements for IF Muting

For non-SNMP-capable upconverters to be used with IF Muting, RF output must be less than -3 dBmV when:

- IF input is absent.
- The switchover time from working to protect is less than one second. That is, when IF is applied to the upconverter, the RF output must be present within one second.

If either of these requirements is not met, the integrity of the N+1 switchover operations could be compromised.

Default Line Card and Bitmap Settings on the Cisco uBR 3x10 RF Switch for Global N+1 Line Card Redundancy

The Cisco uBR 3x10 RF Switch is pre-configured with certain settings to allow plug-and-play with the Cisco uBR10012 universal broadband router for a global 7+1 line card redundancy configuration.

The default bitmap on the Cisco uBR 3x10 RF Switch is 0xFFFFFFFF. This value assumes rfsw-2 on the top half of the Cisco UBR10-MC5X20 BPE, and rfsw-1 on the lower half.

For the protect interface, global configuration uses the IP address of an internal FastEthernet interface.

In 7+1 Redundancy mode, the default header settings are as follows:

- interface 8/0 in header 1
- interface 8/1 in header 2
- interface 7/0 in header 3
- interface 7/1 in header 4

This default setting is based on the line card slot/subslot being configured. The following table lists the mapping of line card interfaces to RF Switch slots (rfsw-slots):

Line Card Slot	5/0	5/1	6/0	6/1	7/0	7/1	8/0	8/1
RFSw-Slot 7+1 mode	7	0	5	6	3	4	1	2

Note Value 0 signifies by default the protect slot. RFSw-Slot header and RF Switch slot # refer to the same thing.

Default Line Card and Bitmap Settings on the Cisco uBR Advanced RF Switch for Global N+1 Line Card Redundancy

Table below shows the default mapping between the slot ID of the Cisco uBR Advanced RF Switch and the line card on the Cisco uBR10012 router.

Table 88: Default Mapping between the Cisco uBR Advanced RF Switch with the Line Card on the Cisco uBR10012 Router

Slot ID on the Cisco uBR Advanced RF Switch	Line Card on the Cisco uBR10012 Router
1	8/0
2	8/1
3	7/0
4	7/1
5	6/0
6	6/1
7	5/0
0	5/1

High Availability Support for Encrypted IP Multicast

The Cisco CMTS router supports 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:

- Dynamic Shared Secret for the Cisco CMTS
- IP Multicast in Cable Networks , White Paper

How to Configure N+1 Redundancy

You must configure and activate both the Cisco RF Switch and the Cisco CMTS to ensure that N+1 redundancy operates correctly.

Note The below configurations are for the Cisco uBR 3x10 RF Switch. For instructions on how to configure the Cisco uBR Advanced RF Switch, see the Cisco uBR Advanced RF Switch Software Configuration Guide .

Common Tasks for Configuring N+1 HCCP Redundancy and Global N+1 Line Card Redundancy

Configuring the Cisco RF Switch for N+1 Redundancy

DETAILED STEPS

	Command or Action	Purpose
Step 1	**set mac address** *mac-address* **Example:** `rfswitch> set mac address 0000.8c01.1111`	(Optional) To specify the MAC address of the Ethernet port on the Cisco RF Switch (used to connect to the LAN), use the set mac address command at the Cisco RF Switch command line interface. The MAC address must be specified using a trio of hexadecimal values. For example, set mac address hex.hex.hex. To negate the existing MAC address assignment and specify a new one, use the no form of this command. If no MAC address is specified, the Cisco RF Switch assumes the default OUI MAC address value.
Step 2	**set ip address** *ip-address* **netmask** [*dhcp*] **Example:** `rfswitch> set ip address 172.16.10.3 255.255.255.0`	(Optional) To specify a static IP address and relative netmask of the Ethernet interface on the Cisco RF Switch, use the set ip address command in User mode. To restore the default setting, user the no form of this command. Default setting differs according to your Firmware Version: • The default IP configuration for Version 3.30 and 3.50 is DHCP enabled. • The dhcp keyword enables the specified IP address as the address for DHCP services on the network. This keyword also produces the same result as the no form of this command for Version 3.30 and 3.50—it enables DHCP. • The default IP configuration for Version 2.50 is the static IP address of 10.0.0.1 255.255.255.0.
Step 3	**set slot config** {*upstreamslots* | *downstreamslots*} **Example:** `Cisco 3x10 RF Switch (default)` `rfswitch> set slot config 0x03ff 0x1c00`	(Optional) Sets the chassis slot-to-line card configuration. The command no set slot config restores the default, which is a 3x10 configuration. Setting a bit position tells the Cisco RF Switch to expect that type of card installed in the slot. A zero in both parameters indicates that the slot should be empty. Both *upstreamslots* and *downstreamslots* are 16-bit hex integer bit-masks that represent whether the slot is enabled/configured for that type of card. The right-most bit represents slot 1. For additional bitmap conversion information, refer to the *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* (Microsoft Excel format) http://www.cisco.com/warp/public/109/BitMap.xls As there are only 14 slots in the Cisco RF Switch chassis, the upper two Most Significant Bits (MSBs) of the 16-bit integer are ignored.

	Command or Action	Purpose
		Note Changes made to the slot configuration on the Cisco RF Switch do not take effect until the system is rebooted (reload command), or an event occurs which causes the enumeration of the chassis line cards to reset.
Step 4	**set snmp community read-write private** **Example:** `rfswitch> set snmp community read-write private`	(Optional) To specify the Simple Network Management Protocol (SNMP) community string on the Cisco RF Switch, use the set snmp community command at the Cisco RF Switch command line interface. This command enables you to gain read and write access to the Cisco RF Switch. The community string must be entered as a string of text. To negate the existing community string and make way for a new one, use the no form of this command. If no SNMP string is entered, the SNMP string assumes the default value private. **Note** Currently, the private keyword is the only SNMP community string supported on communication between the Cisco RF Switch and the Cisco uBR10012 router. The default value of private is the proper setting under normal circumstances.
Step 5	**set snmp host** *ip-address* **Example:** `rfswitch> set snmp host 172.16.10.3`	(Optional) To specify the IP address that receives SNMP notification messages, use the set snmp host command at the Cisco RF Switch command line interface. You can specify more than one SNMP IP address simply by entering this command once for each IP address you want to specify. To negate an existing SNMP IP address assignment, use the no form of this command. If no SNMP IP address is specified, the Cisco RF Switch does not transmit any SNMP notification messages.
Step 6	**set snmp traps** • **Example:** `rfswitch> set snmp traps`	(Optional) To enable SNMP reporting for all modules on the Cisco RF Switch, use the set snmp traps command in the Cisco RF Switch User mode. To deactivate SNMP reporting, use the no form of this command. SNMP reporting is enabled by default on the Cisco RF Switch.
Step 7	**set protection {4|8}** **Example:** `rfswitch> set protection 8`	To set the line card protection scheme, specifying the N+1 protection scheme under which the Cisco RF Switch operates, use the set protection command in Cisco RF Switch User mode. • **set protection4—**Specifies that the Cisco RF Switch operate using a 4+1 protection scheme. • **set protection8—**Specifies that the Cisco RF Switch operate using a 7+1 protection scheme. To negate the existing protection scheme specification, use the no form of this command. The default protection scheme for the Cisco RF Switch is 7+1.
Step 8	**set password** *text* **Example:** `rfswitch> set password cisco`	(Optional) To specify an access password for the Cisco RF Switch command line interface, use the set password command at the Cisco RF Switch command line interface. To negate the existing access password, use the no form of this command.

	Command or Action	Purpose
Step 9	**set tftp-host** *ip-address* **Example:** `rfswitch> set tftp host 172.16.10.17`	(Optional) To specify the host IP address of the TFTP server through which the Cisco RF Switch enables file transfer, use the set tftp-host command at the Cisco RF Switch command line interface. To negate an existing host IP address specification for the remote TFTP server, use the no form of this command. (No default TFTP server IP address is supported on the Cisco RF Switch.)
Step 10	**set switchover-group** *group-name module-bitmap* |**all** **Example:** `rfswitch> set switchover-group a12345 0xAA200000`	To specify a new or existing switchover group name (to which a Cisco RF Switch module is assigned), use the set switchover group command at the Cisco RF Switch command line interface. A switchover group is a collection of Cisco RF Switch interfaces that are all configured to switch over at the same time. • *group-name* — Can be an alpha-numeric string beginning with a non-numeric character. • *module-bitmap* le-bitmap — Defines a Cisco RF Switch module, and must be specified as an eight-character hexadecimal identifier or assigned the all keyword. **Note** Refer to the Creating Cisco RF Switch Module Bitmaps, on page 815 for instructions on creating an appropriate hexadecimal module bitmap. • **all** — Keyword instructs the Cisco RF Switch to automatically switch over all upstream and downstream interfaces connected to the switch module in question. **Note** When setting bit maps on the RF Switch, type 0x in front of the bitmap identifier so that the RF Switch recognizes hexadecimal code. Otherwise, the RF Switch assumes the bitmap is in decimal code. To negate an existing switchover group, use the no set switchover-group command at the Cisco RF Switch command line interface. **Note** You do not need to specify module-bitmap when negating an existing switchover group. For example, the command no set switchover-group a12345 will eliminate the switchover group named “a12345.” Once a switchover group containing one or more Cisco RF Switch modules has been defined, you can use the switch command to enable N+1 redundancy behavior on the Cisco RF Switch, as described in the section Switchover Testing Tasks for N+1 Redundancy, on page 833
Step 11	**save config** **Example:** `rfswitch> save config`	This command saves the latest configuration or image upgrade changes in both Flash and Bootflash, and synchronizes Backup and working copies in each.
Step 12	Choose one of the following:**reboot** • **reboot** • **reload**	This command restarts the Cisco RF Switch so that all changes above take effect.

	Command or Action	Purpose
	Example: `rfswitch>reboot` `or` `rfswitch> reload`	

Operating DHCP with the Cisco RF Switch

DHCP operation is enabled by default, unless the user has set a static IP address using the **set ip address** command in User mode.

When the RF Switch boots, it checks to see if DHCP has been enabled. This is done via the RF Switch commands in a variety of ways. You can use any of the following commands in User mode to enable DHCP:

- **set ip address dhcp**
- **set ip address** *ip-address subnet-mask*
- **no set ip address** (to set the default DHCP operation)

Note The RF Switch Firmware no longer assumes a static IP address of 10.0.0.1 as in versions prior to 3.00. For details on DHCP configuration, see the Cisco RF Switch Firmware Configuration Guide .

Creating Cisco RF Switch Module Bitmaps

Perform the following steps to produce a hexadecimal-format module bitmap that you can then assign to working or protect Cisco RF Switch modules. Module bitmaps for the Cisco RF Switch are comprised of 32-bit map assignments that you translate to an eight-character hexadecimal module bitmap identifier.

Note The Cisco RF Switch ships with some additional pre-configured defaults to ease initial bringup of the switch. For more information on these default settings, see the Default Line Card and Bitmap Settings on the Cisco uBR 3x10 RF Switch for Global N+1 Line Card Redundancy, on page 810.

This procedure cites an example of a typical working cable interface module map with 7+1 redundancy configuration. This scenario connects cable interfaces to the Cisco RF Switch following the example described in the " Cabling " chapter of the Cisco RF Switch Hardware Installation and Configuration Guide :

- Interfaces A, B, C, D, and F comprise the four upstream and one downstream connections to the first MAC domain of a UBR10-LCP2-MC28C cable interface line card installed in a Cisco uBR10012 Series chassis.
- Interfaces H, I, J, K, and M comprise the four upstream and one downstream connections to the second MAC domain on the same cable interface line card.

Note Also refer to the *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* in Microsoft Excel format—available for download and use from Cisco.com.

Step 1 Logically break the two MAC domains up into separate groups and deal with them on their own.
Begin by determining the 32 binary values for the first MAC domain that will eventually define the eight decimal characters leading to the eight hexadecimal characters comprising your module bitmap by laying out the individual bits as follows.

Note In order to optimize N+1 redundancy behavior among the switch modules in the Cisco RF Switch, the internal mapping of the switch circuitry calls for the interfaces to be addressed as they are displayed in the example, below—A H B I C J D K L F M G N.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Step 2 Convert the eight resulting binary quartets into decimal values as follows:
Interim step.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	1 0				1 0				2				0		0				0				0				0					

Step 3 Convert the eight resulting decimal values into hexadecimal values as follows.
The eight resulting hexadecimal characters (in sequence) comprise the eight-character hexadecimal module bitmap for the first MAC domain featuring cable connections to interfaces A, B, C, D, and F on the Cisco RF Switch. Therefore, the resulting module bitmap is AA200000.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	10				10				2				0		0				0				0				0					
Hexadecimal	A				A				2				0		0				0				0				0					

Step 4 Repeat the steps above for the second MAC domain.
Your resulting hexadecimal values should be as follows:

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Binary	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	5				5				1				0				0				0				0				0			
Hexadecimal	5				5				1				0				0				0				0				0			

Therefore, the resulting module bitmap is 55100000.

Note It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure. In such an instance, the combined layout of the two groups exemplified above would be as follows:

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	1	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	15				15				5				0				0				0				0				0			
Hexadecimal	F				F				5				0				0				0				0				0			

After this combination, the resulting module bitmap is FF500000.

Tip Cisco has provided for switchover of an entire cable interface line card by implementing a default module bitmap (referred to by the keyword all) that features an actual hexadecimal module bitmap value of FFFFFFFF.

It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure.

In such an instance, the combined layout of the two groups illustrated above would be as follows:

- If you have a fault on one MAC domain, the other MAC domains will not switch over gracefully merely by toggling the Cisco RF Switch relays. If you have keepalive configured on the other MAC domains, they will eventually switch over, but not efficiently.
- Another method is to have each interface track the other. Therefore, if one interface from a UBR10-LCP2-MC28C cable interface line card goes down, the other interfaces will follow if they have the tracking statement. With this approach, the interface cable 5/0/0 would show the following configuration, for example:

Note Tracking is not needed when using global N+1 configuration. Beginning in Cisco IOS Release 12.3(21)BC, tracking of HCCP interfaces is removed. The **hccp track** command is obsolete.

```
hccp 1 track c5/0/1
```

Interface 5/0/1 would show the following configuration:

```
hccp 2 track c5/0/0
```

Tip We recommend that you disable automatic HCCP revertive functions on both protect downstream channels of a JIB that use keepalive or tracking. Refer to the Disabling HCCP Revertive on Protect Cable Interfaces, on page 832.

Enabling the HCCP Switchover Enhancements Feature

The HCCP Switchover Enhancements feature implements performance improvements for traffic recovery during line card switchover under certain scalability limits.

Within the required network scalability limits, the HCCP Switchover Enhancements feature provides the following switchover benefits:

- Less than 1-second voice call recovery.
- Less than 20-second data recovery.

Prerequisites for the HCCP Switchover Enhancements Feature

- Each line card must support less than 5000 cable modems.
- Each line card must support less than 1000 voice calls.
- The working and protect line cards must have the same channel width.
- The cable line cards must use virtual interface bundling.
- No Layer 3 configuration is supported on the cable interface
- Virtual interface bundling configuration is required to enable the HCCP Switchover Enhancements feature.

Note When you upgrade to Cisco IOS Release 12.2(33)SCA and later, all preexisting cable bundles are automatically converted to virtual bundles, and standalone cable interfaces must be manually configured to be in a virtual bundle. For configuration examples, see Example: Virtual Interface Bundling, on page 874.

Tasks for Configuring Global N+1 Line Card Redundancy

Configuring Global N+1 Line Card Redundancy

Starting with Cisco IOS Release 12.2(33)SCF, you can configure a card with a lower license as the protect card for a working card with a higher license. This protect card remains in a nonfunctional mode (not in standby mode) and does not become active until it is upgraded and reloaded with a higher license, when a switchover occurs.

Before You Begin

- This High Availability configuration describes one or two Cisco RF Switches in the scheme.
- DHCP must be accounted for prior to or during this procedure. An external DHCP server must be installed and operational on the network, or an internal DHCP server must be operational within the

Cisco router. The DHCP server configuration, of either type, must have the following DHCP and DNS entries. Two Cisco RF Switches are illustrated for example:

- Be sure to configure the RF switch name using the **rf-switch name** line card redundancy configuration command, and the RF switch IP addresses prior to configuring line card redundancy.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**ip host rf-sw1***ip_addr* **Example:** `Router(config)# ip host rf-sw1 10.4.4.1`	Assigns the Domain Name System (DNS) entry to the first or only Cisco RF switch in the redundancy scheme.
Step 4	**ip host rf-sw2***ip_addr* **Example:** `Router(config)# ip host rf-sw2 10.4.4.2`	(Required when using two Cisco RF Switches) Assigns the DNS entry to the second Cisco RF switch in the redundancy scheme.
Step 5	**redundancy** **Example:** `Router(config)# redundancy` `Router(config-red)#`	Enables global N+1 redundancy for cases in which factory-configured N+1 redundancy has been disabled, and enters redundancy configuration mode. This command is supported in Cisco IOS Release 12.3(13a)BC and later releases.
Step 6	**linecard-group 1 cable** **Example:** `Router(config-red)# linecard-group 1 cable`	This command assigns the HCCP group to all interfaces on the cable interface line card, or Cisco Broadband Processing Engine.
Step 7	**member subslot** *slot/card* **working** **Example:** `Router(config-red)# member subslot 8/0 working`	This command configures all interfaces on the specified line card to function as HCCP working interfaces in the redundancy scheme. Repeat this step for each working line card in the Cisco router.
Step 8	Do one of the following: • **member subslot** *slot* /*card* **protect**	Configures all interfaces on the specified line card to function as HCCP protect interfaces in the redundancy scheme.

	Command or Action	Purpose
	• **member subslot** *slot /card* **protectconfig***slot /card* **Example:** `Router(config-red)#  member subslot 8/1 protect` `or` `Router(config-red)# member subslot 8/1 protect config 8/0`	For faster switchover results, configures the protect interface for the most appropriate working interface configuration.
Step 9	**end** **Example:** `Router(config-red)# end` `Router#`	Exits global and redundancy configuration modes and returns to Privileged EXEC mode.
Step 10	**write memory** **Example:** `Router# write memory`	After configuring all domains, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Configuring DHCP to Assign IP Addresses on the Cisco RF Switch

To support global N+1 line card redundancy, you must configure either your external DHCP server, or the internal DHCP server on the Cisco uBR10012 universal broadband router to provide the appropriate IP addressing for the Cisco RF switch.

The DHCP server configuration requires the following forms of DHCP and DNS settings:

```
ip dhcp pool rfswitch-pool
      network ...
   !
   ip dhcp pool rfsw-1  [ DHCP MAC->IP mapping for RF-switch # 1 ]
     host a.b.c.d <mask>
     client-id 01aa.bbcc.ddee.ff
   !
   ip dhcp pool rfsw-2  [ DHCP MAC->IP mapping for RF-switch # 2 ]
     host b.c.d.f <mask>
     client-id 01aa.bbcc.ddee.ff
```

You also need to configure DNS entry for each RF-switch, as follows:

```
   ip host rfsw-1 a.b.c.d  [ DNS mapping IP to RF-switch name for rfsw 1 and 2 ]
   ip host rfsw-2 b.c.d.f
```

The following example shows a sample DNS and DHCP configuration on the Cisco uBR10012 universal broadband router for the Cisco RF switch:

```
   ip host rfsw-1 10.10.107.202
   ip host rfsw-2 10.10.107.203
   ip dhcp pool rfsw-1
      host 10.10.107.202 255.255.255.254
```

```
   client-identifier 0003.8f00.0019
!
ip dhcp pool rfswitch-pool
   network 10.10.107.200 255.255.255.252
   next-server 10.10.107.101
   default-router 10.10.107.101
   option 7 ip 10.10.107.101
   option 2 hex ffff.8f80
   option 4 ip 10.10.107.101
   lease infinite
!
ip dhcp pool rfsw-2
   host 10.10.107.203 255.255.255.254
   client-identifier 0003.8f00.0020
!
```

The sample configuration above provides a mechanism to make sure that rfsw-1 only gets IP address 10.10.107.202, and rfsw-1 only gets DHCP IP address 10.10.107.203.

Note The DNS entries for the Cisco RF Switch should be configured before any line card redundancy configuration is attempted.

Enabling Line Card Switchover in Redundancy Mode

The Cisco CMTS router enables switchover on an entire line card at one time, instead of one interface at a time. To switch over a cable interface line card in redundancy mode, use the following command in privileged EXEC mode:

```
Router# redundancy linecard-group switchover from

working-slot
/
working-subslot
```

Note This command switches over a working slot only when active, but not when in protect mode. Also, this command does not switch over the locked interfaces.

To revert to original working and protect status, use the following command in privileged EXEC mode:

```
Router# redundancy linecard-group revertback
working-slot
/
working-subslot
```

This command reverts interfaces from the protect subslot to specified working subslot. If the protect subslot is not active, or is active for some other working subslot, then this command aborts and displays a system error message.

Locking a Switchover for all Interfaces

To lock or unlock a switchover for all interfaces on a given subslot, use the redundancy linecard-group command in privileged EXEC mode:

This command creates a wrapper that locks and unlocks switchover events on all interfaces for the given subslot (for example, interface 5/0). This command only locks or unlocks HCCP interfaces when in working slots.

Note To remove an HCCP configuration from a working or protect interface, use the member subslot command in line card redundancy configuration mode after locking the interface using the redundancy linecard-group command.

For example, to lock the cable line card switchover (set the lockout flag to TRUE), use the following command:

Router# **redundancy linecard-group lockout 5/0**

To force switchover on a locked interface, use the cable power command in privileged EXEC mode.

Enabling Service Internal on HCCP Protect and Standby Working Interfaces

In Cisco IOS Release 12.3(33)SCC and later, to modify the configuration on an HCCP protect and standby working cable interfaces, use the **service internal** command in global configuration mode.

Note When **service internal** command is disabled, you can only change the configuration of an active working interface. The protect line card does not become active directly when it starts up due to hardware reset, or power off/on or other reasons. It will always go to standby state after startup. We recommend that you do not enable **service internal** on the standby working controller, wideband and intergrated cable interfaces of a line card.

Changing Default RF Switch Subslots for Global N+1 Line Card Redundancy

The **member subslot** command enables you to configure a non-default 7+1 wiring other than factory settings. This command supports the option to cable any line card to any RF Switch slot. For example, interface 7/0 might need to be wired to RF Switch slot 7 (instead of the default 3).

To change the factory configuration of subslot mapping to a custom (non-default) mapping, do the following:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.

	Command or Action	Purpose
Step 4	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. • *1*—Line card group number. • **cable**—Specifies the redundancy type.
Step 5	**member subslot***slot* / *subslot* **working rfsw-slot** [*slot-number*] **Example:** `Router(config-red-lc)# member subslot 7/0 working rfsw-slot 7`	Changes the factory configuration of subslot mapping to a custom (non-default) mapping. • *slot* —Chassis slot number of the cable interface line card. The valid range is from 5 to 8. • *subslot* —(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1. • **working**—Specifies the working slot in the line card group. • **rfsw-slot** [*slot-number*]—(Optional) Specifies the RF switch slot for the working line card.
Step 6	**end** **Example:** `Router(config-red-lc)# end`	Returns to privileged EXEC mode.

Changing the Default RF Switch Name and SNMP Community String

The default RF Switch names (rfsw-1 for switch 1 and rfsw-2 for switch 2) are used to perform a DNS lookup for the RF-Switch IP address.

If on an external DHCP server, the RF-Switch DNS names are to be different from the default names, then you need to enter the new RF Switch name as part of line card redundancy configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.
Step 4	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. • *1*—Line card group number. • **cable**—Specifies the redundancy type.
Step 5	**rf-switch name {1|2}** *name* **Example:** `Router(config-red-lc)# rf-switch name {1|2} switch5`	Changes the default RF switch name. • *name* —Alphanumeric name to replace the default name of the Cisco RF Switch.
Step 6	**rf-switch snmp-community community-name** **Example:** `Router(config-red-lc)# rf-switch snmp-community RFswitchstring`	Changes the default SNMP community string. This command updates the Cisco uBR10012 SNMP software only and does not update the new snmp RW community string into the RF Switch. So the user must get into the RF Switch via telnet and set the new snmp RW community string in there. • *community-name* —SNMP community string name.
Step 7	end **Example:** `Router(config-red-lc)# end`	Returns to privileged EXEC mode.

Removing Global N+1 Redundancy Configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**redundancy linecard-group lockout** *slot /subslot*	Locks a line card switchover from the specified working slot and subslot.

	Command or Action	Purpose
	Example: `Router# redundancy linecard-group lockout 6/1`	• *slot*—Chassis slot number of the cable interface line card. The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1.
Step 3	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 4	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.
Step 5	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. • *1*—Line card group number. • **cable**—Specifies the redundancy type.
Step 6	**no member subslot***slot* /*subslot* **working** **Example:** `Router(config-red-lc)# no member subslot 6/1 working`	Removes the specified line card from the global redundancy configuration. • *slot*—Chassis slot number of the cable interface line card. The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1.
Step 7	end **Example:** `Router(config-red-lc)# end`	Returns to privileged EXEC mode.

Tasks for Configuring N+1 HCCP Redundancy

Note Global configuration procedures render interface-level configuration of **hccp** commands obsolete. Legacy HCCP configuration and the newer global N+1 redundancy configuration are mutually exclusive.

Configuring HCCP Groups

This procedure defines HCCP working and protect interfaces for N+1 HCCP Redundancy.

Note When the Cisco CMTS CLI descriptions include the term channel switch, this term refers to the Cisco RF Switch. When configuring HCCP on the Cisco uBR10012 router, use the IP address from the local loopback interface as the working interface IP address. We recommend that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface's IP address to the HCCP protect configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**hccp** *group* **working** *member-id* **Example:** `Router(config-if)# hccp 1 working 1`	Designates a cable interface on a CMTS in the specified HCCP group to be a working CMTS. The hccp working command is to be used for working line card interfaces only. • *group* —The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	**hccp** *group* **protect***member-idip-address* **Example:** `Router(config-if)# hccp 1 protect 2 10.10.10.1`	Assigns the HCCP group number, defines the corresponding HCCP member, and defines the working IP address of the interface used for HCCP communication. The hccp protect command is to be used for protect line card interfaces only.

	Command or Action	Purpose
		Note Working and protect line cards are located on the same Cisco uBR10012 router chassis. In the latter case, we recommend that you use the Loopback IP address in this configuration.
Step 6	**hccp** *group* **channel-switch** *member-id upconverter name* **wavecom-xx** *protect-upconverter-ip-address module working-ip-address its-module* **Example:** `Router(config-if)# hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14`	Configures the upconverter (UPx) topology so that the Vecima upconverter becomes part of the specified HCCP member in a particular HCCP group. **Note** This procedure is not required when configuring N+1 redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20 BPE. **Note** Steps 6 and 7 of this procedure are required for both the working and the protect interfaces.
Step 7	**hccp group channel-switch member-id rf-switch-name rfswitch-group** *ip address* **module-bitmap position** **Example:** `Router(config-if)# hccp 1 channel-switch 2 rfswitch-name rfswitch-group 10.97.1.20 AA200000 2`	Configures the Cisco CMTS so that the specified Cisco RF Switch becomes part of the specified HCCP member in a particular HCCP group. • *ip address* — The IP address of the Cisco RF Switch. • — Specifies the name of the Cisco RF Switch, and must also include the hexadecimal module-bitmap argument. See the Creating Cisco RF Switch Module Bitmaps, on page 815 for instructions on creating an appropriate hexadecimal module bitmap. • **position —** This value specifies the slot/header of the Cisco RF Switch—there are eight on the Cisco uBR10012. **Note** Steps 6 and 7 of this procedure are required for both the working and the protect interfaces.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns to global configuration mode.
Step 9	**write memory** **Example:** `Router# write memory`	After configuring all domains, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Enabling HCCP Protect Interfaces for N+1 Switchover

To enable HCCP protect interfaces, making them available for N+1 switchover should the HCCP working interfaces fail, use the no shutdown command in interface configuration mode on each HCCP protect interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0` `Router(config-if)#`	Ensure that you specify the variables for an HCCP protect interface to enter the interface configuration mode of that protect interface. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the HCCP protect interface.
Step 5	Repeat	Repeat steps 3-4 for every HCCP protect interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns you to global configuration mode.
Step 7	**write memory** **Example:** `Router#  write memory`	After enabling all HCCP protect interfaces, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces

- Before removing HCCP configuration from an active working interface, either shut down the protect or lockout switchover functions using the hccp lock command in interface configuration mode. Otherwise the protect interface will declare the working interface to have failed and will attempt to switch over.
- Do not remove HCCP configuration from an active protect interface. The active member should be restored to its corresponding working interface before removing HCCP configuration from the protect interface.

Note This restriction does not apply when removing HCCP configuration from a protect interface while it is in standby mode and N+1 redundancy is in normal working mode.

To prevent cable modems from going offline during removal of HCCP configuration (on working interfaces), we recommend using one of the following three procedures as a best practice:

Shutting Down HCCP Protect Interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the specified interface. This does not remove interface configuration—merely disables it.

	Command or Action	Purpose
Step 5	Repeat.	Repeat the above steps 3 and 4 as required to shut down all Protect HCCP interfaces.

Locking out HCCP Interface Switchover

Use the hccp lockout command to prevent a working HCCP interface from automatically switching to a protect interface in the same group. This command locks out the HCCP interface. To remove the lockout, use the hccp unlockout command in privileged EXEC mode (re-enabling N+1 redundancy on the working interface).

Note The **hccp lockout** command is not supported starting with Cisco IOS Release 12.2(33)SCE.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hccp** *group* **lockout** *member-id* **Example:** `Router# hccp 1 lockout 1`	To prevent a working HCCP interface from automatically switching to a Protect interface in the same group, use the hccp lockout command in privileged EXEC mode. This command disables HCCP for the specified member of the specified group. • *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive. **Note** Even if an HCCP member is locked out, it switches over in circumstances in which it is tracking another HCCP interface. This condition applies when HCCP interfaces are configured manually to track each other, or when HCCP interfaces share the same JIB, such as with the Cisco UBR10-MC 5X20.
Step 3	Repeat.	Repeat the above steps as required to prevent a working interface from switching over. This manual override can be removed when desired, and retains HCCP configuration on the interface.
Step 4	**hccp** *group* **unlockout** *member* **Example:** `Router# hccp 1 unlockout 1`	Disables the HCCP lockout feature when desired

Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces

Before You Begin

Restriction Starting with Cisco IOS Release 12.2(33)SCC and later, interface level HCCP configuration is not supported. The below configuration step is supported on Cisco IOS Release 12.2(33)SCB and earlier.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**no hccp** *group* {**working** | **protect**} *member-id* **Example:** `Router(config-if)# no hccp 1 protect 1`	Turns off HCCP, and removes the specified HCCP configuration from the specified interface. • *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	Repeat.	Repeat the above steps as required to remove HCCP configuration from all desired HCCP protect interfaces.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Disabling HCCP Revertive on Protect Cable Interfaces

The cable interface line cards pair up interfaces that share the same JIB (ASIC processor). As a result, when HCCP keepalive is enabled on paired DS channels, both DS channels in the pair switch over together if either DS channel has a keepalive failure. For example, if HCCP is configured on DS channels 0 and 1, and DS channel 0 has a keepalive failure, then DS channel 1 also fails because it shares the same JIB with DS channel 0.

When HCCP revertive is enabled on both downstream channels in the pair, the interface that experiences the keepalive failure does not revert automatically to active state. This is desirable behavior because it prevents reverting to active state prematurely—before the cause of an external failure is confirmed and remedied.

The default HCCP revertive time for HCCP interfaces is 30 minutes.

However, the JIB companion interface may act upon the default revertive time of 30 minutes. The companion interface attempts to revert to active state after 30 minutes (when HCCP revertive is enabled). This creates conflict with the failed companion interface on the same JIB.

Note Therefore, we recommend that you disable automatic HCCP revertive functions on both protect downstream channels of a JIB that use keepalive or tracking. If you have keepalive and tracking enabled, or you are using the UBR10-MC 5X20 in N+1 configuration, disable the revertive function on both protect interfaces.

To disable the HCCP revertive function on protect interfaces, do the following:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**nohccp** *group* **revertive**	Disables the automatic HCCP revertive function on the protect interface.

	Command or Action	Purpose
	Example: `Router(config-if)# no hccp 2 revertive`	• *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

What to Do Next

After configuring the redundancy scheme, you can refer to these additional sections:

Switchover Testing Tasks for N+1 Redundancy

Each of these switchover test methods below provides an opportunity to test N+1 redundancy on your Cisco uBR10012 router. Each test method results in the cable modems dropping connectivity temporarily, but staying online, with switchover to protect line cards and interfaces.

Electromagnetic relays can develop a magnetic charge over time that could interfere with normal operations. Therefore, Cisco Systems recommends periodic testing using these procedures to ensure smooth operation. The tests in this section help to improve overall system availability.

These switchover testing tasks apply to switchover from HCCP working interfaces to HCCP protect interfaces, or vice versa, when configured in N+1 redundancy.

Pre-testing System Check Procedures

As a best practice, we strongly recommend analyzing the CMTS headend status prior to switchover testing.

Caution Switchover testing with latent configuration or status problems can create disruptions in subscriber service.

Use these pre-test system checks prior to manual switchover testing:

Displaying HCCP Working and HCCP Protect Interface Status

To display a brief summary of the HCCP groups, configuration types, member numbers, and status for cable interfaces, use the **show hccp brief** command at the Cisco uBR 3x10 RF Switch prompt. rfswitch> **show hccp brief**

```
Interface Config    Grp Mbr Status
Ca5/0/0   Protect   1   3   standby
Ca7/0/0   Working   1   3   active
```

Displaying HCCP Group Status on the Cisco CMTS

As a best practice, we recommend that you perform this test prior to performing any manual switchovers. This status check verifies stable redundancy operations. Should this procedure reveal any problems with online states, resolve these problems prior to performing a manual switchover. Otherwise, manual switchover for testing purposes might create additional problems.

To display HCCP group status on the Cisco CMTS, including Cisco RF Switch information relevant to N+1 redundancy behavior, use the show hccp channel-switch command in privileged EXEC mode. This command displays status for all channel switches belonging to the specified HCCP group and HCCP member. For details on the sample output the show hccp channel-switch command, see the Example: Channel Switch Information from the Cisco uBR10012 Router, on page 843.

Displaying Cisco RF Switch Module Status on the Cisco uBR 3x10 RF Switch

As a best practice, we recommend that you perform this pretest status check prior to performing any manual switchovers. This status check confirms the online and administrative states for all modules on the Cisco uBR 3x10 RF Switch itself.

To display current module status for one or more modules on the Cisco uBR 3x10 RF Switch, use the show module all command at Cisco uBR 3x10 RF Switch prompt. For details on the show module all command sample output, see Example: Cisco 3x10 RF Switch Modules in 7+1 Mode, on page 840.

Switchover Testing Procedures

The first two procedure below describe how to test the performance of N+1 redundancy on your Cisco CMTS headend. The final procedure describes how to analyze Cisco CMTS headend status after switchover.

Testing Cisco RF Switch Relays with Manual Switchover

We recommend testing the switch relays once a week (optimal) and at least once a month (minimal). Perform these steps to test the working RF Switch relays with switchover to protect.

Tip You can toggle the relays on the switch without affecting the upconverter or any of the modems. This is important if testing the relays without actually switching any of the line cards or the corresponding upconverters. If a relay is enabled on the switch and a fail-over occurs, it will go to the proper state and not just toggle from one state to another.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**telnet ip-address /noecho** **Example:** `Router# telnet 172.16.10.3 /noecho`	Initiate configuration by connecting to the Cisco RF Switch using the console or by using a Telnet session. Either provides CLI access for initiating a switchover. If a Telnet password is set on the Cisco RF Switch, type password string, where string is the previously-defined password set on the RF Switch. The Telnet password is set using the separate set password string command in Cisco RF Switch User mode. **Note** To prevent multiple users from changing the Firmware configuration at any one time, only a single Telnet client connection can be opened at a time, regardless of whether this connection is password-protected. Telnet access to the RF Switch from the router console makes double entries when typing. One workaround is to disable local echo. For example, from the Cisco uBR10012 router CLI, use the /noecho option (as shown at left).

	Command or Action	Purpose
		Common Telnet disconnect methods are as follows: • Press Ctrl+Break. • Press Ctrl+]. • Type quit or send break. Another Telnet disconnect method is as follows: • Press Ctrl+Shift 6 6 x. • Type disc 1 from the router CLI. For additional Telnet break sequences, refer to the document Standard Break Key Sequence Combinations During Password Recovery on Cisco.com.
Step 2	Do one of the following: • **test module** • **switch group-name** *x* **Example:** `rfswitch> test module` `or` `rfswitch> switch 13 1`	The test module command tests all the relays at once, and then returns to the normal working mode. **Caution** Do not use the test module command while in the protect mode. Alternately, you can test an entire bitmap with switch group-name x, where x is the RF Switch header number. For example, the switch 13 1 tests port G on slot 1 of the Cisco RF Switch.
Step 3	switch group-name 0 **Example:** `rfswitch> switch 13 0`	Use the command switch group name 0 (or idle) to disable the relays, and to return to normal working mode.

Testing HCCP Groups with Manual Switchover

Cisco Systems recommends that you perform a periodic CLI switchover test of an HCCP group from the CMTS to test the protect card and path. However, this type of switchover may take 4-6 seconds and could cause a small percentage of modems to go offline. Therefore, this test should be performed less often than previous tests, and only during off-peak hours.

SUMMARY STEPS

1. **enable**
2. **hccp** *group* **switch** *member*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hccp** *group* **switch** *member* **Example:** `Router# hccp 1 switch 1`	Manually switches a working CMTS with its protect CMTS peer (or vice versa).

Using the show cable modem Command After a Manual Switchover

If you are using HCCP 1+1 or N+1 redundancy, the new primary processor after a switchover automatically creates a new database of the online cable modems. Use the following procedure to force IP traffic and to display cable modem status and information.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable modem** *ip-address* **Example:** `Router# show cable modem 172.16.10.3` `MAC Address IP Address I/F MAC Prim RxPwr Timing Num BPI` `State Sid (db) Offset CPE Enb` `0000.3948.ba56 8.60.0.8 C6/0/0/U0 online 1 0.50 2138 0 N`	Identifies the IP address of a specific cable modem to be displayed. You can also specify the IP address for a CPE device behind a cable modem, and information for that cable modem is displayed.
Step 3	**ping ip-address** **Example:** `Router# ping 172.16.10.3`	Forces IP traffic by sending an ICMP ECHO packet.

Verifying N+1 Redundancy Configuration

The following example of the show running configuration command illustrates the N+1 redundancy scheme configured on the Cisco uBR10012 router with two Cisco uBR 3x10 RF Switches:

```
Router# show running config
...
redundancy
 linecard-group 1 cable
  rf-switch name 1 rfsw1
  rf-switch name 2 rfsw2
  rf-switch protection-mode [4+1/7+1]
  rf-switch snmp-community private123
  revertive <1-35791>
  member subslot 5/0 working
  member subslot 5/1 protect
  member subslot 8/1 working
  member subslot 5/1 protect config 8/1
  mode sso
...
```

The following is a sample output of the show redundancy linecard all command in privileged EXEC mode for Global N+1 Line Card Redundancy. This redundancy configuration supports two Cisco uBR 3x10 RF Switches on the Cisco CMTS router.

```
Router# show redundancy linecard all
 hccp config sync list:
 end
 Don't generate default PHY config configuration: FALSE
 User defined PHY config configuration: FALSE
 Redundancy Mode: 7 + 1
 Linecard Redundancy Detail
 --------------------------
Card      Config   Mbr RfSw-Name       RfSw-IP-Addr    RfSw-Slot Bitmap
card 8/0  Working  80  rfsw-2          5.37.0.20       8         0xFFFFFFFF
card 8/0  Working  80  rfsw-1          5.37.0.19       8         0xFFFFFFFF
card 7/0  Working  70  rfsw-2          5.37.0.20       7         0xFFFFFFFF
card 7/0  Working  70  rfsw-1          5.37.0.19       7         0xFFFFFFFF
 Subslot Summary
--------------------
                              RF Switch Slot*
   Subslot        Status      Current         Default
 ------------------------------------------------------------
    5/0           Unknown       -               7
    5/1           Unknown       -               P
    6/0           Unknown       -               5
    6/1           Unknown       -               6
    7/0           Working       7               3
    7/1           Unknown       -               4
    8/0           Working       8               1
    8/1           Unknown       -               2
 ------------------------------------------------------------------
 NOTE:
 Legend: - = Unused; P= Protect
```

The following is a sample output of the show redundancy linecard all command in privileged EXEC mode for N+1 HCCP Redundancy. This redundancy configuration supports two Cisco uBR 3x10 RF Switches on the Cisco router.

```
Router# show redundancy linecard all
Interface Config   Grp Mbr RfSw-Name       RfSw-IP-Addr    RfSw-Slot Bitmap
Ca6/1/0   Working  1   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/1   Working  2   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/2   Working  3   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/2   Working  3   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca6/1/3   Working  4   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca6/1/4   Working  5   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
```

```
Ca7/0/0   Protect  1   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca7/0/0   Protect  1   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca7/0/1   Protect  2   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca7/0/1   Protect  2   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca7/0/2   Protect  3   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca7/0/2   Protect  3   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
Ca7/0/2   Protect  3   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca7/0/2   Protect  3   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca7/0/3   Protect  4   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
Ca7/0/3   Protect  4   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca7/0/4   Protect  5   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
Ca7/0/4   Protect  5   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca8/0/0   Working  1   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca8/0/1   Working  2   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca8/0/2   Working  3   80  rfsw-1          10.4.4.1        1         0xFFFFFFFF
Ca8/0/2   Working  3   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
Ca8/0/3   Working  4   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
Ca8/0/4   Working  5   80  rfsw-2          10.4.4.2        1         0xFFFFFFFF
```

In addition to the show redundancy linecard all command illustrated above, you can use the following command to display additional redundancy information for a specified slot:

- **show redundancy linecard all | incCa8/0/1**

The following table summarizes HCCP group and member information that is assigned to HCCP configuration on the Cisco CMTS. These factory-configured settings configure the Cable slot/subslot interfaces on the router, and supporting slot configuration on the Cisco uBR 3x10 RF Switches in either 4+1 or 7+1 redundancy.

Table 89: HCCP Member Numbers for Cisco uBR10012 Slots/ Subslots in Global N+1 Redundancy

Downstream Number	Group Number	8/0	8/1	7/0	7/1	6/0	6/1	5/0	5/1
DS 0	1	80	81	70	71	60	61	50	P1
DS 1	2	80	81	70	71	60	61	50	P1
DS 2	3	80	81	70	71	60	61	50	P1
DS 3	4	80	81	70	71	60	61	50	P1
DS 4	5	80	81	70	71	60	61	50	P1
Default RF Switch Slot (7+1 Mode)	1	2	3	4	5	6	7	P1	
Default RF Switch Slots (4+1 Mode)	5, 1	6, 2	7, 3	8, 4	-	-	-	P1, P2	

Configuration Examples for Cisco N+1 Redundancy

This section provides the following configuration examples of N+1 redundancy. Each chassis-level example below illustrates a distinct implementation of N+1 redundancy on the Cisco CMTS.

Note For configuration examples for the Cisco uBR Advanced RF Switch, see Cisco uBR Advanced RF Switch Software Configuration Guide .

Table 90: Summary Table of N+1 Configuration Examples—Cisco IOS 12.2(15)BC2a, Firmware 3.50

Example	Cisco RF Switch[55]	N+1 Mode	Cisco Router Chassis[56]	Cisco Cable Interface Line Cards
Cisco RF Switch Module Examples				
Example: Cisco 3x10 RF Switch Modules in 7+1 Mode, on page 840	3x10 RF	7+1[57]	uBR10012	Not described
Cisco uBR10012 Chassis Configuration Examples				
Examples: N+1 HCCP Redundancy in 4+1 Mode, on page 841	3x10 RF	4+1	uBR10012	UBR10-MC 5X20 (five)
Example: Channel Switch Information from the Cisco uBR10012 Router, on page 843	3x10 RF	7+13	uBR10012	Not described
Example: Global N+1 Redundancy Using the Cisco uBR-MC3GX60V Line Card , on page 856	3x10 RF (two)	7+13	uBR10012	uBR-MC3GX60V
Example: Global N+1 Redundancy Using the Cisco UBR10-MC5X20 Line Card , on page 862	3x10 RF (two)	7+13	uBR10012	UBR10-MC 5X20

Example	Cisco RF Switch[55]	N+1 Mode	Cisco Router Chassis[56]	Cisco Cable Interface Line Cards
Example: Global N+1 Redundancy Using the Cisco UBR10-LCP2-MC28C Line Card, on page 869	3x10 RF	7+13	uBR10012	UBR10-LCP2-MC28C (eight)

55 Assume one Cisco RF Switch per example unless more are cited.

56 Assume one Cisco router chassis per example unless more are cited.

57 The term "7+1 Redundancy" is also referred to as "8+1 Redundancy" in the field—physically, eight line cards in "8+1" mode are configured as seven working line cards with one protect line card. Therefore, "7+1 Redundancy" is the more physically accurate term. By contrast, "4+1 Redundancy" (predictably) refers to four working line cards with one additional protect line card.

Example: Cisco 3x10 RF Switch Modules in 7+1 Mode

The following is sample output for the **show module all** command from a Cisco RF Switch that has been configured for 7+1 Redundancy:

```
rfswitch> show module all
SNMP Cache: enabled
Module  Presence  Admin  Cache  Fault
     1    online      0      0     ok
     2    online      0      0     ok
     3    online      0      0     ok
     4    online      0      0     ok
     5    online      0      0     ok
     6    online      0      0     ok
     7    online      0      0     ok
     8    online      0      0     ok
     9    online      0      0     ok
    10    online      0      0     ok
    11    online      0      0     ok
    12    online      0      0     ok
    13    online      0      0     ok
    14   offline      0      0     ok
```

The Administrative State field (Admin) indicates the following potential states:

- 0 — Indicates normal working state.
- 1-8 — Indicates that there has been a switchover and the corresponding module is in protect mode, and the header is being protected. For example, an Admin state of 8 for Module 1 would indicate a switchover for port A (Module 1) on header 8 on the Cisco RF Switch. After a switchover, verify that this Admin state corresponds with the actual wiring on the Cisco RF Switch.
- 9—Indicates fault for the specified module.

The following is sample output of the **show config** command from a Cisco 3x10 RF Switch configured in 7+1 Redundancy mode:

```
rfswitch> show config
IP addr: 10.74.59.242
Subnet mask: 255.255.255.192
MAC addr: 00-03-8F-01-13-BB
Gateway IP: 10.74.59.193
TFTP host IP: 20.4.0.2
```

```
ARP timeout: 14400 secs
DHCP lease time: infinite
TELNET inactivity timeout: 600 secs
TELNET echo mode: on
Password: (none)

SNMP Community: private
SNMP Cache: enabled
SNMP Traps: enabled
SNMP Trap Interval: 300 sec(s)
SNMP Trap Hosts: none
Card Protect Mode: 8+1
Protect Mode Reset: disabled
Slot Config: 0x03ff 0x1c00 (13 cards)
Watchdog Timeout: 20 sec(s)
Group definitions: 1
  ALL        0xffffffff
```

Note The show config command for the Cisco RF Switch contains the Card Protect Mode field. When this field displays 8+1 , this indicates that the Cisco RF Switch is configured for N+1 redundancy, where eight or less working line cards are possible. This field may also display 4+1 , where four or less working line cards are possible.

Examples: N+1 HCCP Redundancy in 4+1 Mode

The following output from the Cisco IOS show running configuration command illustrates the configuration of N+1 redundancy using the following CMTS:

- One Cisco 3x10 RF Switch configured as two working RF Switches in 4+1 mode
- One Cisco uBR10012 router
- Five Cisco UBR10-MC 5X20 broadband processing engines

The Protection mode affects the bitmaps of the Cisco RF Switch and CMTS configuration.

Note If you add one additional Cisco UBR10-MC 5X20 BPE, the entire CMTS configuration below must be changed. Refer to the cabling in the following document for additional information:

- Cabling the Cisco UBR10-MC 5X20 Cable Interface Line Card

http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/quick/start/MC52_cbl.html

Example: HCCP Working 1

The following configuration example illustrates HCCP working member 1 for five HCCP groups:

```
interface c8/0/0
hccp 1 working 1
hccp 1 channel-switch 1 rfswa rfswitch-group 10.10.10.10 44440400 1
interface c8/0/1
hccp 2 working 1
hccp 2 channel-switch 1 rfswa rfswitch-group 10.10.10.10 11110100 1
interface c8/0/2
hccp 3 working 1
```

```
hccp 3 channel-switch 1 rfswa rfswitch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfswb rfswitch-group 10.10.10.10 0000a080 1
interface c8/0/3
hccp 4 working 1
hccp 4 channel-switch 1 rfswb rfswitch-group 10.10.10.10 88880800 1
interface c8/0/4
hccp 5 working 1
hccp 5 channel-switch 1 rfswb rfswitch-group 10.10.10.10 22220200 1
```

Example: HCCP Working 2

The following configuration example illustrates HCCP working member 2 for five HCCP groups:

```
interface c8/1/0
hccp 1 working 2
hccp 1 channel-switch 2 rfswa rfswitch-group 10.10.10.10 44440400 2
interface c8/1/1
hccp 2 working 2
hccp 2 channel-switch 2 rfswa rfswitch-group 10.10.10.10 11110100 2
interface c8/1/2
hccp 3 working 2
hccp 3 channel-switch 2 rfswa rfswitch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfswb rfswitch-group 10.10.10.10 0000a080 2
interface c8/1/3
hccp 4 working 2
hccp 4 channel-switch 2 rfswb rfswitch-group 10.10.10.10 88880800 2
interface c8/1/4
hccp 5 working 2
hccp 5 channel-switch 2 rfswb rfswitch-group 10.10.10.10 22220200 2
```

Example: HCCP Working 3

The following configuration example illustrates HCCP working member 3 for five HCCP groups:

```
interface c7/0/0
hccp 1 working 3
hccp 1 channel-switch 3 rfswa rfswitch-group 10.10.10.10 44440400 3
interface c7/0/1
hccp 2 working 3
hccp 2 channel-switch 3 rfswa rfswitch-group 10.10.10.10 11110100 3
interface c7/0/2
hccp 3 working 3
hccp 3 channel-switch 3 rfswa rfswitch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfswb rfswitch-group 10.10.10.10 0000a080 3
interface c7/0/3
hccp 4 working 3
hccp 4 channel-switch 3 rfswb rfswitch-group 10.10.10.10 88880800 3
interface c7/0/4
hccp 5 working 3
hccp 5 channel-switch 3 rfswb rfswitch-group 10.10.10.10 22220200 3
```

Example: HCCP Working 4

The following configuration example illustrates HCCP working member 4 for five HCCP groups:

```
interface c7/1/0
hccp 1 working 4
hccp 1 channel-switch 4 rfswa rfswitch-group 10.10.10.10 44440400 4
interface c7/1/1
hccp 2 working 4
hccp 2 channel-switch 4 rfswa rfswitch-group 10.10.10.10 11110100 4
interface c7/1/2
hccp 3 working 4
hccp 3 channel-switch 4 rfswa rfswitch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfswb rfswitch-group 10.10.10.10 0000a080 4
```

```
interface c7/1/3
hccp 4 working 4
hccp 4 channel-switch 4 rfswb rfswitch-group 10.10.10.10 88880800 4
interface c7/1/4
hccp 5 working 4
```

HCCP Protect Interface Configuration Examples

The following examples illustrate the four HCCP protect members for five HCCP groups:

```
interface c5/1/0
hccp 1 protect 1 10.10.10.1
hccp 1 channel-switch 1 rfswa rfswitch-group 10.10.10.10 44440400 1
hccp 1 protect 2 10.10.10.1
hccp 1 channel-switch 2 rfswa rfswitch-group 10.10.10.10 44440400 2
hccp 1 protect 3 10.10.10.1
hccp 1 channel-switch 3 rfswa rfswitch-group 10.10.10.10 44440400 3
hccp 1 protect 4 10.10.10.1
hccp 1 channel-switch 4 rfswa rfswitch-group 10.10.10.10 44440400 4
interface c5/1/1
hccp 2 protect 1 10.10.10.1
hccp 2 channel-switch 1 rfswa rfswitch-group 10.10.10.10 11110100 1
hccp 2 protect 2 10.10.10.1
hccp 2 channel-switch 2 rfswa rfswitch-group 10.10.10.10 11110100 2
hccp 2 protect 3 10.10.10.1
hccp 2 channel-switch 3 rfswa rfswitch-group 10.10.10.10 11110100 3
hccp 2 protect 4 10.10.10.1
hccp 2 channel-switch 4 rfswa rfswitch-group 10.10.10.10 11110100 4
interface c5/1/2
hccp 3 protect 1 10.10.10.1
hccp 3 channel-switch 1 rfswa rfswitch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfswb rfswitch-group 10.10.10.10 0000a080 1
hccp 3 protect 2 10.10.10.1
hccp 3 channel-switch 2 rfswa rfswitch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfswb rfswitch-group 10.10.10.10 0000a080 2
hccp 3 protect 3 10.10.10.1
hccp 3 channel-switch 3 rfswa rfswitch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfswb rfswitch-group 10.10.10.10 0000a080 3
hccp 3 protect 4 10.10.10.1
hccp 3 channel-switch 4 rfswa rfswitch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfswb rfswitch-group 10.10.10.10 0000a080 4
interface c5/1/3
hccp 4 protect 1 10.10.10.1
hccp 4 channel-switch 1 rfswb rfswitch-group 10.10.10.10 88880800 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfswb rfswitch-group 10.10.10.10 88880800 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfswb rfswitch-group 10.10.10.10 88880800 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfswb rfswitch-group 10.10.10.10 88880800 4
interface c5/1/4
hccp 5 protect 1 10.10.10.1
hccp 5 channel-switch 1 rfswb rfswitch-group 10.10.10.10 22220200 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfswb rfswitch-group 10.10.10.10 22220200 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfswb rfswitch-group 10.10.10.10 22220200 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfswb rfswitch-group 10.10.10.10 22220200 4
```

Example: Channel Switch Information from the Cisco uBR10012 Router

The following is a sample output of the show hccp channel-switch command that provides information about the channel switch activity with Global N+1 Line Card Redundancy:

```
Router# show hccp channel-switch
Grp 1 Mbr 70 Working channel-switch:
```

```
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 2 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 3 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
```

```
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 4 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 5 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 6 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
```

```
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 7 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 8 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
```

```
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 9 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 10 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 11 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
```

```
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 12 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 13 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
```

```
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 14 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 15 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 1 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
```

```
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 2 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 3 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
```

```
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 4 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 5 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 6 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
```

```
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 7 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 8 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
```

```
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 9 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 10 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 11 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
```

```
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 12 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 13 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
```

```
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 14 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 15 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
RFswitch relay test in 2w5d
RFswitch polling count = 2585/0
```

The following is a sample output of the show hccp channel-switch command that provides information about the channel switch activity with N+1 HCCP Redundancy:

```
Router# show hccp channel-switch
Grp 1 Mbr 1 Working channel-switch:
 "uc" - enabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
Grp 2 Mbr 1 Working channel-switch:
  "uc" - enabled, frequency 555000000 Hz
  "rfswitch" - module 2, normal
  module 4, normal
  module 6, normal
  module 9, normal
  module 13, normal
Grp 1 Mbr 7 Protect channel-switch:
 "uc" - disabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
Grp 1 Mbr 5 Protect channel-switch:
 "uc" - disabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
```

Example: Global N+1 Redundancy Using the Cisco uBR-MC3GX60V Line Card

The following output from the show run command illustrates the configuration of N+1 redundancy in remote learn DEPI mode on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco uBR-MC3GX60V line cards:

Router# show run

```
!
On the Cisco CMTS router
!
card 5/1 ubr10k-clc-3g60 license 72X60
card 7/1 ubr10k-clc-3g60 license 72X60
card 8/1 ubr10k-clc-3g60 license 72X60
l2tp-class l2tp_class_gi7_1
!
l2tp-class l2tp_class_gi8_1
depi-class depi_class_gi7_1
 mode mpt
!
depi-class depi_class_gi8_1
 mode mpt
!
depi-tunnel gi7_1
 dest-ip 60.3.2.9
 l2tp-class l2tp_class_gi7_1
 depi-class depi_class_gi7_1
 protect-tunnel qam5_pt
!
depi-tunnel gi8_1
 dest-ip 60.3.2.13
 l2tp-class l2tp_class_gi8_1
 depi-class depi_class_gi8_1
 protect-tunnel qam5_pt
```

```
!
depi-tunnel qam5_pt
 dest-ip 60.6.2.13

redundancy
 linecard-group 1 cable
  rf-switch protection-mode 4+1
  rf-switch name 1 rfsw1
  member subslot 5/1 protect
  member subslot 7/1 working rfsw-slot 2
  member subslot 8/1 working rfsw-slot 3
  member subslot 5/1 protect config 7/1
  mode sso
!
controller Modular-Cable 7/1/0
 rf-channel 0 cable downstream channel-id 9
 rf-channel 0 frequency 303000000 annex B modulation 256qam interleave 32
 rf-channel 0 depi-tunnel gi7_1 tsid 38009
 rf-channel 0 rf-power 52.0
 no rf-channel 0 rf-shutdown
 rf-channel 1 cable downstream channel-id 10
 rf-channel 1 frequency 309000000 annex B modulation 256qam interleave 32
 rf-channel 1 depi-tunnel gi7_1 tsid 38010
 rf-channel 1 rf-power 52.0
 no rf-channel 1 rf-shutdown
 rf-channel 2 cable downstream channel-id 11
 rf-channel 2 frequency 315000000 annex B modulation 256qam interleave 32
 rf-channel 2 depi-tunnel gi7_1 tsid 38011
 rf-channel 2 rf-power 52.0
 no rf-channel 2 rf-shutdown
 rf-channel 3 cable downstream channel-id 12
 rf-channel 3 frequency 321000000 annex B modulation 256qam interleave 32
 rf-channel 3 depi-tunnel gi7_1 tsid 38012
 rf-channel 3 rf-power 52.0
 no rf-channel 3 rf-shutdown
 rf-channel 4 cable downstream channel-id 13
 rf-channel 4 frequency 327000000 annex B modulation 256qam interleave 32
 rf-channel 4 depi-tunnel gi7_1 tsid 38013
 rf-channel 4 rf-power 52.0
 no rf-channel 4 rf-shutdown
 rf-channel 5 cable downstream channel-id 14
 rf-channel 5 frequency 333000000 annex B modulation 256qam interleave 32
 rf-channel 5 depi-tunnel gi7_1 tsid 38014
 rf-channel 5 rf-power 52.0
 no rf-channel 5 rf-shutdown
 rf-channel 6 cable downstream channel-id 15
 rf-channel 6 frequency 339000000 annex B modulation 256qam interleave 32
 rf-channel 6 depi-tunnel gi7_1 tsid 38015
 rf-channel 6 rf-power 52.0
 no rf-channel 6 rf-shutdown
 rf-channel 7 cable downstream channel-id 16
 rf-channel 7 frequency 345000000 annex B modulation 256qam interleave 32
 rf-channel 7 depi-tunnel gi7_1 tsid 38016
 rf-channel 7 rf-power 52.0
 no rf-channel 7 rf-shutdown
 rf-channel 8 cable downstream channel-id 81
 rf-channel 9 cable downstream channel-id 82
 rf-channel 10 cable downstream channel-id 83
 rf-channel 11 cable downstream channel-id 84
 rf-channel 12 cable downstream channel-id 85
 rf-channel 13 cable downstream channel-id 86
 rf-channel 14 cable downstream channel-id 87
 rf-channel 15 cable downstream channel-id 88
 rf-channel 16 cable downstream channel-id 89
 rf-channel 17 cable downstream channel-id 90
 rf-channel 18 cable downstream channel-id 91
 rf-channel 19 cable downstream channel-id 92
 rf-channel 20 cable downstream channel-id 93
 rf-channel 21 cable downstream channel-id 94
 rf-channel 22 cable downstream channel-id 95
 rf-channel 23 cable downstream channel-id 96
!
controller Modular-Cable 8/1/0
```

```
 rf-channel 0 cable downstream channel-id 17
 rf-channel 0 frequency 351000000 annex B modulation 256qam interleave 32
 rf-channel 0 depi-tunnel gi8_1 tsid 38017
 no rf-channel 0 rf-shutdown
 rf-channel 1 cable downstream channel-id 18
 rf-channel 1 frequency 357000000 annex B modulation 256qam interleave 32
 rf-channel 1 depi-tunnel gi8_1 tsid 38018
 no rf-channel 1 rf-shutdown
 rf-channel 2 cable downstream channel-id 19
 rf-channel 2 frequency 363000000 annex B modulation 256qam interleave 32
 rf-channel 2 depi-tunnel gi8_1 tsid 38019
 no rf-channel 2 rf-shutdown
 rf-channel 3 cable downstream channel-id 20
 rf-channel 3 frequency 369000000 annex B modulation 256qam interleave 32
 rf-channel 3 depi-tunnel gi8_1 tsid 38020
 no rf-channel 3 rf-shutdown
 rf-channel 4 cable downstream channel-id 21
 rf-channel 4 frequency 375000000 annex B modulation 256qam interleave 32
 rf-channel 4 depi-tunnel gi8_1 tsid 38021
 no rf-channel 4 rf-shutdown
 rf-channel 5 cable downstream channel-id 22
 rf-channel 5 frequency 381000000 annex B modulation 256qam interleave 32
 rf-channel 5 depi-tunnel gi8_1 tsid 38022
 no rf-channel 5 rf-shutdown
 rf-channel 6 cable downstream channel-id 23
 rf-channel 6 frequency 387000000 annex B modulation 256qam interleave 32
 rf-channel 6 depi-tunnel gi8_1 tsid 38023
 no rf-channel 6 rf-shutdown
 rf-channel 7 cable downstream channel-id 24
 rf-channel 7 frequency 393000000 annex B modulation 256qam interleave 32
 rf-channel 7 depi-tunnel gi8_1 tsid 38024
 no rf-channel 7 rf-shutdown
 rf-channel 8 cable downstream channel-id 81
 rf-channel 9 cable downstream channel-id 82
 rf-channel 10 cable downstream channel-id 83
 rf-channel 11 cable downstream channel-id 84
 rf-channel 12 cable downstream channel-id 85
 rf-channel 13 cable downstream channel-id 86
 rf-channel 14 cable downstream channel-id 87
 rf-channel 15 cable downstream channel-id 88
 rf-channel 16 cable downstream channel-id 89
 rf-channel 17 cable downstream channel-id 90
 rf-channel 18 cable downstream channel-id 91
 rf-channel 19 cable downstream channel-id 92
 rf-channel 20 cable downstream channel-id 93
 rf-channel 21 cable downstream channel-id 94
 rf-channel 22 cable downstream channel-id 95
 rf-channel 23 cable downstream channel-id 96
!
interface Cable7/1/0
 downstream Modular-Cable 1/0/0 rf-channel 0 upstream 0-3
 downstream Modular-Cable 7/1/0 rf-channel 0 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 1
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 cable upstream 0 attribute-mask 20000000
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 16400000
```

```
 cable upstream 1 channel-width 6400000 6400000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 1
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 cable upstream 1 attribute-mask 20000000
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 23800000
 cable upstream 2 channel-width 6400000 6400000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 1
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 30200000
 cable upstream 3 channel-width 6400000 6400000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 1
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
!
interface GigabitEthernet7/1/0
 ip address 60.3.2.10 255.255.255.252
 negotiation auto
!
interface Modular-Cable7/1/0:0
 cable bundle 1
 cable rf-bandwidth-percent 36
!
interface Wideband-Cable7/1/0:3
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
!
interface Wideband-Cable7/1/0:4
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
!
interface Wideband-Cable7/1/0:8
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
 cable rf-channel 4 bandwidth-percent 20
 cable rf-channel 5 bandwidth-percent 20
 cable rf-channel 6 bandwidth-percent 20
 cable rf-channel 7 bandwidth-percent 20
!
interface Cable8/1/0
 downstream Modular-Cable 1/0/0 rf-channel 1 upstream 0-3
 downstream Modular-Cable 8/1/0 rf-channel 0 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 1
  upstream 0
```

```
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 1
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 cable upstream 0 attribute-mask 20000000
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 16400000
 cable upstream 1 channel-width 6400000 6400000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 1
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 cable upstream 1 attribute-mask 20000000
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 23800000
 cable upstream 2 channel-width 6400000 6400000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 1
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 30200000
 cable upstream 3 channel-width 6400000 6400000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 1
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
interface GigabitEthernet8/1/0
 ip address 60.3.2.14 255.255.255.252
 negotiation auto
!
interface Modular-Cable8/1/0:0
 cable bundle 1
 cable rf-bandwidth-percent 36
!
interface Wideband-Cable8/1/0:3
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
!
interface Wideband-Cable8/1/0:4
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
!
interface Wideband-Cable8/1/0:8
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
```

```
 cable rf-channel 4 bandwidth-percent 20
 cable rf-channel 5 bandwidth-percent 20
 cable rf-channel 6 bandwidth-percent 20
 cable rf-channel 7 bandwidth-percent 20
!
interface Bundle1
 ip address 30.0.42.1 255.255.255.0 secondary
 ip address 30.0.43.254 255.255.255.0 secondary
 ip address 30.0.44.254 255.255.255.0 secondary
 ip address 30.0.41.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 cable dhcp-giaddr policy
 cable helper-address 20.1.0.9
!
On the Cisco RF Switch
!
l2tp-class l2tp_class_gi7_1
l2tp-class l2tp_class_gi8_1
depi-class depi_class_gi7_1
 mode mpt
depi-class depi_class_gi8_1
 mode mpt
depi-tunnel gi8_1
 dest-ip 60.3.2.14
 l2tp-class l2tp_class_gi8_1
 depi-class depi_class_gi8_1
 protect-tunnel qam5_pt
!
depi-tunnel gi7_1
 dest-ip 60.3.2.10
 l2tp-class l2tp_class_gi7_1
 depi-class depi_class_gi7_1
 protect-tunnel qam5_pt
!
depi-tunnel qam5_pt
 dest-ip 60.6.2.14
interface GigabitEthernet5/14
 no switchport
 ip address 60.3.2.9 255.255.255.252 secondary
 ip address 60.3.2.13 255.255.255.252
 no ip redirects
!
interface Qam5/3.1
 cable mode depi remote learn
 cable downstream tsid 38009
 depi depi-tunnel gi7_1
!
interface Qam5/3.2
 cable mode depi remote learn
 cable downstream tsid 38010
 depi depi-tunnel gi7_1
!
interface Qam5/3.3
 cable mode depi remote learn
 cable downstream tsid 38011
 depi depi-tunnel gi7_1
!
interface Qam5/3.4
 cable mode depi remote learn
 cable downstream tsid 38012
 depi depi-tunnel gi7_1
!
interface Qam3/5.1
 cable mode depi remote learn
 cable downstream tsid 38013
 depi depi-tunnel gi7_1
!
interface Qam3/5.2
 cable mode depi remote learn
 cable downstream tsid 38014
```

```
 depi depi-tunnel gi7_1
!
interface Qam3/5.3
 cable mode depi remote learn
 cable downstream tsid 38015
 depi depi-tunnel gi7_1
!
interface Qam3/5.4
 cable mode depi remote learn
 cable downstream tsid 38016
 depi depi-tunnel gi7_1
!
interface Qam5/1
 no ip address
!
interface Qam5/1.1
 cable mode depi remote learn
 cable downstream tsid 38017
 depi depi-tunnel gi8_1
!
interface Qam5/1.2
 cable mode depi remote learn
 cable downstream tsid 38018
 depi depi-tunnel gi8_1
!
interface Qam5/1.3
 cable mode depi remote learn
 cable downstream tsid 38019
 depi depi-tunnel gi8_1
!
interface Qam5/1.4
 cable mode depi remote learn
 cable downstream tsid 38020
 depi depi-tunnel gi8_1
!
interface Qam5/2
 no ip address
!
interface Qam5/2.1
 cable mode depi remote learn
 cable downstream tsid 38021
 depi depi-tunnel gi8_1
!
interface Qam5/2.2
 cable mode depi remote learn
 cable downstream tsid 38022
 depi depi-tunnel gi8_1
!
interface Qam5/2.3
 cable mode depi remote learn
 cable downstream tsid 38023
 depi depi-tunnel gi8_1
!
interface Qam5/2.4
 cable mode depi remote learn
 cable downstream tsid 38024
 depi depi-tunnel gi8_1
!
```

Example: Global N+1 Redundancy Using the Cisco UBR10-MC5X20 Line Card

The following output from the show run command illustrates configuration of N+1 redundancy on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco UBR10-MC 5X20 line cards:

```
Router# show run
Current configuration : 8567 bytes
!
version 12.2
no parser cache
```

```
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-15.BC1
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
!
!  Use this modulation profile if using current released BC3 IOS and 16-QAM is required.
!  A-TDMA IOS has different modulation profiles and requirements.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
 frequency 453000000
 service-class 1 max-upstream 10000
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1522
!
redundancy
  main-cpu
    auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigethernet-1
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 5/0 5cable-mc520s-d
card 5/1 5cable-mc520s-d
card 6/0 5cable-mc520s-d
card 6/1 5cable-mc520s-d
card 7/0 5cable-mc520s-d
card 7/1 5cable-mc520s-d
card 8/0 5cable-mc520s-d
card 8/1 5cable-mc520s-d
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
!  This is set for console access from the 10012 router to the Switch.
!  The IP address is for Loopback0.
!
ip dhcp pool MODEMS1
   network 172.25.1.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.1.1
   default-router 172.25.1.1
   option 7 ip 172.25.1.1
   option 4 ip 172.25.1.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp pool MODEMS2
   network 172.25.2.0 255.255.255.0
```

```
   bootfile docsis.cm
   next-server 172.25.2.1
   default-router 172.25.2.1
   option 7 ip 172.25.2.1
   option 4 ip 172.25.2.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
!  An internal DHCP server is used in this example instead of external servers
!  (cable helper, TOD, TFTP, etc.).  External servers are recommended in a genuine
!  production network.
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
 ip address 10.97.1.8 255.255.255.0
 ip rip receive version 2
 no ip split-horizon
 no keepalive
!
interface GigabitEthernet1/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet2/0/0
 no ip address
 negotiation auto
!
!  Sample Interface Config for N+1: (This assumes rfsw2 is on the top as shown in
!  the RF Switch Cabling document).  Other interfaces will be the same except a
!  different member number for each HCCP group.
!
interface Cable5/1/0
!
!  This is the Protect interface for the first HCCP group.  It may be best to configure
!  the Protect interface(s) last; after the Working interfaces are configured,
!  or to keep the interface "shut" (disabled) until all configurations are completed.
!
 no ip address
!
!  There is no need to set the IP address because it comes from the Working card via SNMP.
!
 no keepalive
!
!  This is defaulted to 10 seconds with the N+1 IOS code, but should be disabled on
!  the Protect interface or set relatively high.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
!
!  The DS modulation and Interleave must be the same on the Protect and Working interfaces
 !  of the same HCCP group. The Protect interface itself must be "no shut" (enabled)
!  for HCCP to activate
!
 cable downstream rf-shutdown
 cable upstream 0 shutdown
!
!  These interfaces automatically become "no shut" (enabled) when a switchover occurs.
!
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 hccp 1 protect 1 10.10.10.1
!
!  This is the first HCCP group and it is protecting member 1 with member 1's
!  FE IP address.  If it is intra-chassis, you can use the Loopback0 IP address.
!
 hccp 1 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 AA200000 1
!
```

```
!  This is the IP address of the RF Switch and it is protecting member 1, which
!  has a bitmap of AA200000 in Switch slot 1.
!
 hccp 1 protect 2 10.10.10.1
!
!  This is the first HCCP group and it is protecting member 2 with the loopback
!  IP address.
!
 hccp 1 channel-switch 2 rfsw2 rfswitch-group 10.97.1.20 AA200000 2
!
!  This is the IP address of the RF Switch and it is protecting member 2, with a
!  bitmap of AA200000 in Switch slot 2.
!
 hccp 1 protect 3 10.10.10.1
 hccp 1 channel-switch 3 rfsw2 rfswitch-group 10.97.1.20 AA200000 3
 hccp 1 protect 4 10.10.10.1
 hccp 1 channel-switch 4 rfsw2 rfswitch-group 10.97.1.20 AA200000 4
 hccp 1 protect 5 10.10.10.1
 hccp 1 channel-switch 5 rfsw2 rfswitch-group 10.97.1.20 AA200000 5
 hccp 1 protect 6 10.10.10.1
 hccp 1 channel-switch 6 rfsw2 rfswitch-group 10.97.1.20 AA200000 6
 hccp 1 protect 7 10.10.10.1
 hccp 1 channel-switch 7 rfsw2 rfswitch-group 10.97.1.20 AA200000 7
!
!  These channel-switch configurations can be copied and pasted into their respective
!  Working interfaces.
!
 hccp 1 timers 5000 15000
!
!  Cisco IOS command = hccp 1 timers <hellotime> <holdtime>
!  This is mostly for inter-chassis communication, so set it high for the uBR10012
!  as this can create extra CPU load.
!
 no hccp 1 revertive
!
interface Cable5/1/1
!
!  This is the Protect interface for the second group.
!
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 !
 hccp 2 protect 1 10.10.10.1
 hccp 2 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 55100000 1
!
!  Because this MAC domain is on right side of header, the bitmap in
!  hexadecimal code is 55100000.
!
 hccp 2 protect 2 10.10.10.1
 hccp 2 channel-switch 2 rfsw2 rfswitch-group 10.97.1.20 55100000 2
 hccp 2 protect 3 10.10.10.1
 hccp 2 channel-switch 3 rfsw2 rfswitch-group 10.97.1.20 55100000 3
 hccp 2 protect 4 10.10.10.1
 hccp 2 channel-switch 4 rfsw2 rfswitch-group 10.97.1.20 55100000 4
 hccp 2 protect 5 10.10.10.1
 hccp 2 channel-switch 5 rfsw2 rfswitch-group 10.97.1.20 55100000 5
 hccp 2 protect 6 10.10.10.1
 hccp 2 channel-switch 6 rfsw2 rfswitch-group 10.97.1.20 55100000 6
 hccp 2 protect 7 10.10.10.1
 hccp 2 channel-switch 7 rfsw2 rfswitch-group 10.97.1.20 55100000 7
 hccp 2 timers 5000 15000
 no hccp 2 revertive
interface Cable5/1/2
!
!  This is the Protect interface for the third group.
```

```
!
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 hccp 3 protect 1 10.10.10.1
 hccp 3 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 00C80000 1
 hccp 3 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 00C00000 1
!
!  Because the third MAC domain will traverse both Switches, two statements are needed.
!  The "00" in front of the bitmaps are dropped when viewing the running configuration.
!
 no hccp 3 revertive
interface Cable5/1/3
!
!  This is the Protect interface for the fourth group.
!
 hccp 4 protect 1 10.10.10.1
 hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
 hccp 4 protect 2 10.10.10.1
 hccp 4 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 AA200000 2
 hccp 4 protect 3 10.10.10.1
 hccp 4 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 AA200000 3
 hccp 4 protect 4 10.10.10.1
 hccp 4 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 AA200000 4
 hccp 4 protect 5 10.10.10.1
 hccp 4 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 AA200000 5
 hccp 4 protect 6 10.10.10.1
 hccp 4 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 AA200000 6
 hccp 4 protect 7 10.10.10.1
 hccp 4 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 AA200000 7
 no hccp 4 revertive
.
interface Cable5/1/4
!
!  This is the Protect interface for the fifth group.
!
 hccp 5 protect 1 10.10.10.1
 hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
 hccp 5 protect 2 10.10.10.1
 hccp 5 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 55100000 2
 hccp 5 protect 3 10.10.10.1
 hccp 5 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 55100000 3
 hccp 5 protect 4 10.10.10.1
 hccp 5 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 55100000 4
 hccp 5 protect 5 10.10.10.1
 hccp 5 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 55100000 5
 hccp 5 protect 6 10.10.10.1
 hccp 5 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 55100000 6
 hccp 5 protect 7 10.10.10.1
 hccp 5 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 55100000 7
.
.
.
!  Interface configurations continue as such for the remaining Protect interfaces.
!
interface Cable8/1/0
!
!  This is the Working interface for the first group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.1.1 255.255.255.0
!
!  Interface bundling is supported as are subinterfaces.
!
 ip rip send version 2
 ip rip receive version 2
```

```
 keepalive 1
!
!  The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!  Only set this value after modems have stabilized.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
!
!  This is the DS frequency, which must be set for the internal upconverter to operate.
!
 cable downstream channel-id 0
 no cable downstream rf-shutdown
!
!  This is needed to turn on the DS RF output.
!
 cable upstream 0 frequency 24000000
!
!  If doing dense mode combining, the upstream frequencies will need to be different.
!  If no two US ports are shared, the same frequency can be used.
!
 cable upstream 0 power-level 0
 cable upstream 0 connector 0
!
cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 22
 no cable upstream 0 shutdown
.
.
.
 cable dhcp-giaddr policy
!
!  This tells cable modems to get an IP address from the primary scope and CPEs to use
!  the secondary scope.
!
 hccp 1 working 1
!
!  This is Working member 1 of HCCP Group 1.
!
hccp 1 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of Switch & member 1, which has a bitmap of
!  AA200000 in Switch slot 1.
!
 hccp 1 reverttime 120
!
!  This is the time in minutes (+ 2 minute suspend) for the card to switch back to
!  normal mode if the fault has cleared.  If a fault was initiated by a keepalive
!  and you had a fault on the Protect card, it would revert back after the suspend
!  time and not wait the full revert time.
!
interface Cable8/1/1
!
!  This is the Working interface for the second HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.2.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 1
 no cable downstream rf-shutdown
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 cable upstream 0 connector 4
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 22
```

```
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
.
.
.
 cable dhcp-giaddr policy
 hccp 2 working 1
!
!  This is Working member 1 of HCCP Group 2.
!
 hccp 2 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 55100000 1
!
!  This is the IP address of Switch & Member 1 of Group 2, which has a bitmap of
!  55100000 in Switch slot 1.
!
 hccp 2 reverttime 120
!
interface Cable8/1/2
!
!  This is the Working interface for the third HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.3.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 2
 no cable downstream rf-shutdown
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 cable upstream 0 connector 8
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 22
 no cable upstream 0 shutdown
 cable dhcp-giaddr policy
.
.
.
 hccp 3 working 1
!
!  This is the Working member 1 of HCCP Group 3.
!
 hccp 3 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 00c80000 1
 hccp 3 channel-switch 1 rfsw2 rfswitch-group 10. 97.1.20 00c00000 1
 hccp 3 reverttime 120
interface Cable8/1/3
!
!  This is the Working interface for the fourth HCCP group.
!
 hccp 4 working 1
 hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
 hccp 4 reverttime 120
interface Cable8/1/4
!
!  This is the Working interface for the fifth HCCP group.
!
 hccp 5 working 1
 hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
 hccp 5 reverttime 120
!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
!  This does not affect the HCCP communications between the Switch and uBR10012.
!
```

```
snmp-server enable traps cable
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
alias exec t configure terminal
alias exec scm show cable modem
alias exec scr sh cab mode remote
alias exec shb sh hccp br
alias exec shd sh hccp detail
alias exec shc sh hccp chan
!
line con 0
 logging synchronous
line aux 0
 no exec
 transport input all
!
!  The three lines above were used to console from the Auxiliary port of the uBR10012
!  to the Switch.
!
line vty 0 4
 session-timeout 400
 password xx
 login
endBuilding configuration...
```

Example: Global N+1 Redundancy Using the Cisco UBR10-LCP2-MC28C Line Card

The following output from the show run command illustrates configuration of N+1 redundancy on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco UBR10-LCP2-MC28C line cards:

```
Router# show run
Current configuration : 8567 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-4.BC1b
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
 frequency 453000000
 service-class 1 max-upstream 10000
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1522
!
redundancy
  main-cpu
    auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigethernet-1
```

```
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 5/0 2cable-mc28c
card 5/1 2cable-mc28c
card 6/0 2cable-mc28c
card 6/1 2cable-mc28c
card 7/0 2cable-mc28c
card 7/1 2cable-mc28c
card 8/0 2cable-mc28c
card 8/1 2cable-mc28c
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
!  This is set for console access from the uBR10012 router to the RF Switch.
!  The IP address is for Loopback0.
!
ip dhcp pool MODEMS1
   network 172.25.1.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.1.1
   default-router 172.25.1.1
   option 7 ip 172.25.1.1
   option 4 ip 172.25.1.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp pool MODEMS2
   network 172.25.2.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.2.1
   default-router 172.25.2.1
   option 7 ip 172.25.2.1
   option 4 ip 172.25.2.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
!  An internal DHCP server was used for testing in this example instead of external
!  servers (cable helper, TOD, TFTP, etc.).  External servers are recommended in a
!  genuine production network.
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
 ip address 10.97.1.8 255.255.255.0
 ip rip receive version 2
 no ip split-horizon
 no keepalive
!
interface GigabitEthernet1/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet2/0/0
 no ip address
 negotiation auto
!
interface Cable5/1/0
!
!  This is the Protect interface for the first group.  Remember to configure the
!  Protect interface(s) last; after the Working interfaces are configured.
!
 no ip address
!
!  There is no need to set the IP address because it comes from the Working card via SNMP.
!
 no keepalive
!
!  This is set by default to 10 seconds with the N+1 IOS code, but should be disabled
!  on the Protect interface or set to be relatively high.
```

```
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
!
!  The DS modulation and Interleave depth must be same on Protect and Working interfaces
!  of the same group.
!
 cable upstream 0 shutdown
!
!  This automatically becomes "no shut" (enabled) when a switchover occurs.
!
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
 hccp 1 protect 1 10.10.10.1
!
!  This is the HCCP first group and it is protecting member 1 with member 1's
!  FE IP address.  If it's intra-chassis, you can use the Loopback0 IP address.
!
 hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
!  This is the IP address of upconverter and its module 2 (B) that is backing
!  module 16 (P) of the upconverter.  This shows that one upconverter could have
!  a module backing up a module in a different chassis with a different IP address
!  if need be.  If this statement is not present when using 15BC2 IOS and above,
!  IF-Muting is assumed and an external upconverter with snmp capability is not needed.
!
 hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of the Switch and it is protecting member 1, which has a
!  bitmap of AA200000 in Switch slot 1.
!
 hccp 1 protect 2 10.10.10.1
!
!  This is the HCCP first group and it is protecting member 2 with its IP address.
!
 hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14
!
!  This is the IP address of the upconverter and its module 2 (B) that's backing
!  module 14 (N).
!
 hccp 1 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 AA200000 2
!
!  This is the IP address of the Switch and it is protecting member 2, with a
!  bitmap of AA200000 in Switch slot 2.
!
 hccp 1 protect 3 10.10.10.1
 hccp 1 channel-switch 3 uc wavecom-hd 10.97.1.21 2 10.97.1.21 12
 hccp 1 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 AA200000 3
 hccp 1 protect 4 10.10.10.1
 hccp 1 channel-switch 4 uc wavecom-hd 10.97.1.21 2 10.97.1.21 10
 hccp 1 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 AA200000 4
 hccp 1 protect 5 10.10.10.1
 hccp 1 channel-switch 5 uc wavecom-hd 10.97.1.21 2 10.97.1.21 8
 hccp 1 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 AA200000 5
 hccp 1 protect 6 10.10.10.1
 hccp 1 channel-switch 6 uc wavecom-hd 10.97.1.21 2 10.97.1.21 6
 hccp 1 channel-switch 6 rfswitch rfswitch-group 10.97.1.20 AA200000 6
 hccp 1 protect 7 10.10.10.1
 hccp 1 channel-switch 7 uc wavecom-hd 10.97.1.21 2 10.97.1.21 4
 hccp 1 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 AA200000 7
 hccp 1 timers 5000 15000
!
!  Cisco IOS command = hccp 1 timers <hellotime> <holdtime>
!  This is mostly for inter-chassis communication, so set it high for the uBR10012 router
!  as this can create extra CPU load.
!
interface Cable5/1/1
!
!  This is the Protect interface for the second group.
!
```

```
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
!
 hccp 2 protect 1 10.10.10.1
 hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
 hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
!  Because this MAC domain is on right side of header, the bitmap in hexadecimal code
!  is 55100000.
!
 hccp 2 protect 2 10.10.10.1
 hccp 2 channel-switch 2 uc wavecom-hd 10.97.1.21 1 10.97.1.21 13
 hccp 2 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 55100000 2
 hccp 2 protect 3 10.10.10.1
 hccp 2 channel-switch 3 uc wavecom-hd 10.97.1.21 1 10.97.1.21 11
 hccp 2 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 55100000 3
 hccp 2 protect 4 10.10.10.1
 hccp 2 channel-switch 4 uc wavecom-hd 10.97.1.21 1 10.97.1.21 9
 hccp 2 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 55100000 4
 hccp 2 protect 5 10.10.10.1
 hccp 2 channel-switch 5 uc wavecom-hd 10.97.1.21 1 10.97.1.21 7
 hccp 2 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 55100000 5
 hccp 2 protect 6 10.10.10.1
 hccp 2 channel-switch 6 uc wavecom-hd 10.97.1.21 1 10.97.1.21 5
 hccp 2 channel-switch 6 rfswitch rfswitch- group 10.97.1.20 55100000 6
 hccp 2 protect 7 10.10.10.1
 hccp 2 channel-switch 7 uc wavecom-hd 10.97.1.21 1 10.97.1.21 3
 hccp 2 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 55100000 7
 hccp 2 timers 5000 15000
!
interface Cable8/1/0
!
!  This is the Working interface for the first group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.1.1 255.255.255.0
!
!  Interface bundling is supported also as well as subinterfaces.
!
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
!
!  The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
!
!  This is DS frequency, which used to be informational only when using an external
!  upconverter.  This must be set when doing N+1, so the Protect upconverter knows
!  which frequency to use.
!
 cable upstream 0 frequency 24000000
!
!  If doing dense mode combining, the upstream frequencies need to be different.
!  If no two US ports are shared, the same frequency can be used.
!
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
```

```
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
!
!  This tells cable modems to get an IP address from the primary scope and CPEs
!  to use the secondary scope.
!
 hccp 1 working 1
!
!  This is Working member 1 of HCCP Group 1.
!
 hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
!  This is the IP address of the upconverter and its module 2 (B) that's backing
!  module 16 (P).
!
 hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of the Switch & member 1, which has a bitmap of
!  AA200000 in Switch slot 1.
!
 hccp 1 reverttime 120
!
!  This is the time in minutes (+ 2 minute suspend) for the card to switch back to
!  normal mode if the fault has cleared.  If a fault was initiated by a keepalive
!  and you had a fault on the Protect card, it would revert back after the suspend
!  time and not await the full revert time.
!
interface Cable8/1/1
!
!  This is the Working interface for the second HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.2.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
 hccp 2 working 1
!
!  This is Working member 1 of HCCP Group 2.
!
 hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
 hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
!  This is the IP address of the Switch & Member 1 of Group 2, which has a bitmap of
!  55100000 in Switch slot 1.
!
 hccp 2 reverttime 120
!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
!  This does not affect the HCCP communications between the Upconverter, Switch,
!  the and uBR10012.
!
snmp-server enable traps cable
```

```
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
line con 0
 logging synchronous
line aux 0
 no exec
 transport input all
!
!  The three lines above were used to console from the Auxiliary port of the uBR10012
!  to the Switch.
!
line vty 0 4
 session-timeout 400
 password xx
 login
endBuilding configuration...
```

Example: Virtual Interface Bundling

Example of Previously Supported Cable Line Card Interface Configuration Compared With Virtual Interface Bundling Configuration

The following example shows an older cable line card interface configuration with IP addressing:

```
interface cable 5/0/0
ip address 10.10.10.1 255.255.255.0
ip address 10.10.11.1 255.255.255.0 secondary
```

If previously configured on your router, this older cable line card interface configuration is automatically replaced by the following virtual interface bundling configuration, where no IP addressing is supported at the cable line card interface:

```
interface cable 5/0/0
no ip address
cable bundle 1
interface bundle 1
ip address 10.10.10.1 255.255.255.0
ip address 10.10.11.1 255.255.255.0 secondary
```

Example of Previously Supported Master/Slave Bundle Configuration with Virtual Interface Bundling Configuration

The following example shows the older cable line card interface configuration with IP addressing and master/slave bundling:

```
interface cable 5/0/0
ip address 10.10.10.1 255.255.255.0
cable bundle 5 master
interface cable 5/0/1
no ip address
cable bundle 5
```

If previously configured on your router, this older cable line card interface configuration is automatically replaced by the following virtual interface bundling configuration, where no IP addressing is supported at the cable line card interface:

```
interface cable 5/0/0
no ip address
cable bundle 5
interface cable 5/0/1
no ip address
```

```
cable bundle 5
interface bundle 5
ip address 10.10.10.1 255.255.255.0
Additional Information
```

Additional References

For additional information related to N+1 redundancy, the Cisco RF switch, and the Cisco uBR10012 routers, refer to the following references.

Related Documents

Related Topic	Document Title
Command References	• *Cisco IOS CMTS Cable Command Reference, 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html • *Cisco RF Switch Firmware Command Reference Guide* http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html
Cisco RF Switches	• Cisco RF Switch Documentation Home Page (complete documentation set) http://www.cisco.com/en/US/products/hw/cable/ps2929/tsd_products_support_series_home.html
High Availability References for Cisco Broadband Cable	• *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* (Microsoft Excel format)
Additional Broadband Cable Technical Reference	• *Cisco Multiservice Broadband Cable Guide* http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_brochure09186a008014eeb0.pdf • *Cable Radio Frequency (RF) FAQs* http://www.cisco.com/en/US/tech/tk86/tk319/technologies_q_and_a_item09186a0080134faa.shtml

Standards

Standard	Title
DOCSIS	Data-Over-Cable Service Interface Specifications
EuroDOCSIS	European Data-Over-Cable Service Interface Specifications

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for N+1 Redundancy

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

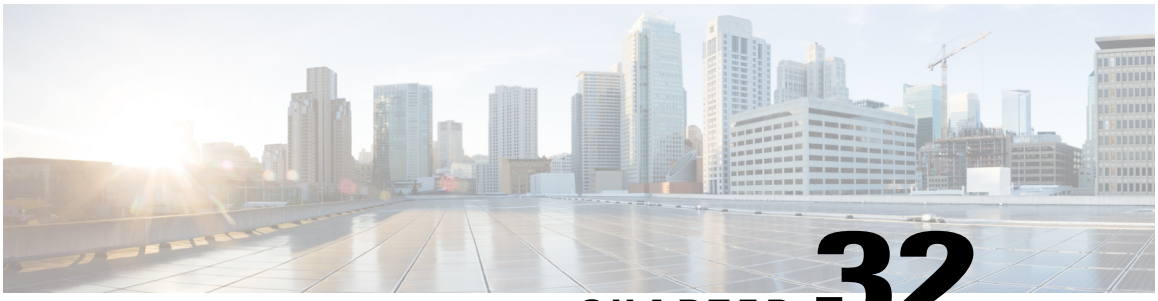
Table 91: Feature Information for N+1 Redundancy

Feature Name	Releases	Feature Information
HCCP N+1 Redundancy	12.1(10)EC	**HCCP support introduced on the Cisco uBR7200 series routers.**
HCCP N+1 Redundancy	12.2(4)XF1, 12.2(4)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router.
HCCP N+1 Redundancy	12.2(15)BC2a	• HCCP N+1 Redundancy support introduced for the Cisco uBR7246VXR router and the Cisco uBR 3x10 RF Switch. • CLI Usability—Synchronizes HCCP interface command-line interface (CLI) configuration between working and protect interfaces. • Support for N+1 redundancy for the Cisco UBR10-MC 5X20 BPE on the Cisco uBR10012 router. • IF Muting on the Cisco CMTS for non-SNMP-Capable Upconverters, on page 808 — enables N+1 redundancy on CMTS headends that do not use SNMP-enabled upconverters.

Feature Name	Releases	Feature Information
Global N+1 Line Card Redundancy	12.3(13a)BC	HCCP N+1 redundancy on the Cisco 7200 series routers is no longer supported. The following enhancements were introduced to HCCP N+1 redundancy support on the Cisco uBR10012 router: • Global N+1 Line Card Redundancy, on page 807 • Automatic running of the show hccp channel switch command for Background Path Testing for HCCP N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router.

Feature Name	Releases	Feature Information
HCCP Switchover Enhancements	12.3(21)BC	The following support has been removed: • HCCP N+1 redundancy support is removed for the Cisco uBR7246VXR router. • Tracking of HCCP interfaces is removed. The **hccp track** command is obsolete. The HCCP Switchover Enhancements feature is introduced on the Cisco uBR10012 router, with the following new support: • Performance improvements for traffic recovery during line card switchover under certain scalability limits. Within the required network scalability limits, the HCCP Switchover Enhancements feature provides the following switchover benefits: ◦ Less than 1-second voice call recovery. ◦ Less than 20-second data recovery. • To prevent false switchovers, the keepalive failure logic is modified. • For faster line card switchovers, the **member subslot protect** command has been modified to add the [**config** *slot*/*subslot*] option. When using the new **config** option, you can preload upstream connectors on an HCCP protected interface to emulate the most common line card connector assignments.

Feature Name	Releases	Feature Information
N+1 Redundancy	12.2(33)SCC	• HCCP N+1 redundancy support introduced on the Cisco uBR10012 router for Cisco uBR-MC 20X20V broadband processing engine (BPE). • Support for Legacy HCCP configurations has been removed. • Enabling Service Internal on HCCP Protect and Standby Working Interfaces, on page 822—The service internal command enables configuration of the protect and standby working cable interfaces for the following line cards: ◦ Cisco uBR10-MC5X20S, Cisco uBR10-MC5X20U, Cisco uBR10-MC5X20H and Cisco UBR-MC20X20V line cards.
N+1 Redundancy	12.2(33)SCE	The config option in the member subslot protect command is made the default. When more than one working card is configured, this option is automatically applied to the first working card.
N+1 Redundancy	12.2(33)SCF	This release supports configuration of a card with a lower license as protect for a working card with a higher license. However, when a switchover occurs, this protect card does not become active until it is upgraded and reloaded with a higher license.
N+1 Redundancy	12.2(33)SCG	Support for the new Cisco uBR Advanced RF Switch was added.



CHAPTER 32

Route Processor Redundancy for the Cisco uBR10012 Universal Broadband Router

First Published: February 14, 2008

Last Updated: January 28, 2013

The Route Processor Redundancy feature for the Cisco CMTS Routers is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Route Processor Redundancy (RPR) reduces unplanned downtime. RPR enables a quicker switchover between active and standby PRE modules in the event of a fatal error on the active PRE module. When you configure RPR, the standby PRE is synchronized with the active PRE. In the event of a fatal error on the active PRE, the system switches to the standby PRE, which reinitializes itself and functions as the active PRE, reducing downtime of the system.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Route Processor Redundancy

- Two PRE modules must be installed in the Cisco uBR10012 chassis.
- The two processor modules must be of the same type. Both modules must be PRE2 modules or both modules must be PRE4 modules. You cannot mix PRE2 and PRE4 modules in the same chassis.
- Both PRE modules must be running identical software releases.
- For full redundancy, the FastEthernet port on the standby PRE module must have its own connection to the network. The console port on the standby PRE module must also be connected to a terminal, either by connecting it to a second terminal or by using a terminal server or other device to connect it to the same terminal used by the PRE module.
- Both PRE modules must be configured with the same amount of onboard SDRAM. A standby PRE cannot come online as the active PRE if the standby PRE has a smaller amount of SDRAM than the active PRE module.

Table below shows the hardware compatibility prerequisites for this feature.

Note Support for Route Processor Redundancy features in Cisco IOS Releases before 12.2BC; however, several of these releases and hardware have since reached End-of-Life (EOL) and therefore only the latest Cisco IOS software release trains are shown in the hardware compatibility table. For more information about the complete feature history, see the Feature Information for Route Processor Redundancy, on page 905.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 92: Route Processor Redundancy for Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5

Restrictions for Route Processor Redundancy

- Both PRE modules must be running Cisco IOS Release 12.2(33)SCA or Cisco IOS Release 12.2 SC releases to support the RPR feature.

Information About Route Processor Redundancy

Cisco IOS Release 12.2(4)XF and Cisco IOS Release 12.2(4)BC introduce support for Route Processor Redundancy (RPR) on the Cisco uBR10012 universal broadband router. The RPR feature enables the Cisco uBR10012 to use two PRE modules in a redundant configuration, so that if the active PRE module fails or becomes inactive, the system automatically performs a *switchover* , where the standby PRE module takes over and assumes full responsibility for systems operations.

Note From Cisco IOS release 12.2SC onwards, Nonstop Forwarding (NSF) and Stateful Switchover (SSO) are recommended and supported on the Cisco uBR10012 router. For SSO configuration details, see the "Configuring SSO" section in the *Stateful Switchover* guide at the following link: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html.

Note Unless otherwise indicated, all references to a PRE module in this document also include the PRE2 or PRE4 modules. However, when using redundant PRE modules, they cannot be mixed but must both be of the same type: both must be PRE2 modules or both must be PRE4 modules.

The RPR feature does not require a full reboot of the system to perform a switchover. When the system is originally initialized, the standby PRE module performs an abbreviated initialization routine—the PRE module performs all self-checks and loads the Cisco IOS software, but instead of performing normal systems operations it begins monitoring the active PRE module. If the standby PRE module detects a failure in the primary module, it can quickly assume the primary responsibility for systems operations.

Each PRE module contains all the resources required to operate the router, such as bootflash memory, Flash disks, Ethernet ports, and console port. In the default operation, the standby PRE module also synchronizes the major systems files, such as the Cisco IOS startup configuration file, so that during a switchover, the standby PRE module can duplicate the active PRE module's configuration. This process also resets the cable and network uplink interfaces.

Note Resetting the Gigabit Ethernet and OC-12 POS line cards will interrupt traffic for approximately 45 seconds. Because of DOCSIS requirements, a reset of the cable interface line cards requires all cable modems to go offline and reregister with the Cisco uBR10012 router. This will interrupt traffic on the cable network for 10 to 15 minutes, depending on the number of customers actually online at the time. A side-effect of this process is that when the cable modems come online again, they will not necessarily be assigned the same Service IDs (SIDs) that they had before the switchover.

Because the standby PRE module is partially initialized, you can use Cisco IOS CLI commands to access its resources, such as the Flash disks and bootflash. For example, you can use the **dir** command to list the contents of a device, or use the **copy** command to transfer files between the primary and standby PRE modules. (See the Using Redundant File Systems, on page 887 for more information on this feature.)

Switchover Procedure

A switchover occurs when the standby PRE module takes over responsibilities from the active PRE module. The switchover can occur automatically if the standby PRE module has determined that the active PRE module has failed, or an operator can initiate a manual switchover whenever desired.

A switchover triggers the following events:

1. If this is a manual switchover, the active PRE module verifies that the standby PRE module is present and is running Cisco IOS software that supports the RPR feature. If so, it instructs the standby PRE module to begin switchover procedures, and the active PRE module either attempts to reload its configured Cisco IOS software image or enters ROM monitor mode, depending on the setting of its configuration register.
2. The standby PRE module completes its initialization procedures, which includes completely loading the Cisco IOS software, verifying the physical components of the Cisco uBR10012 chassis, and parsing the startup configuration file. The standby PRE module is configured identically to the previous active PRE module, including the IP address for its onboard FastEthernet management interface.
3. The standby PRE assumes responsibility as the active PRE module and brings the Cisco uBR10012 chassis into a known state, which includes resetting all installed and enabled line cards and respective interfaces.

Note Resetting the Gigabit Ethernet and OC-12 POS line cards will interrupt traffic for approximately 45 seconds. Because of DOCSIS requirements, the reset of the cable interface line cards requires all cable modems to go offline and reregister with the Cisco uBR10012 router. This will interrupt traffic on the cable network for 10 to 15 minutes, depending on the number of customers actually online at the time. A side-effect of this process is that when the cable modems come online again, they will not necessarily be assigned the same Service IDs (SIDs) that they had before the switchover.

1. The new active PRE module begins normal systems operations, including passing traffic.

Note Depending on the setting of the PRE module's config register, it either reloads the Cisco IOS software or is left in the ROM monitor state. If the PRE module is in the ROM monitor state, it does not begin functioning as a standby PRE module until it is reloaded with the **hw-module sec-cpu reset** command.

Is PRE Switchover Failing?

The usual phenomenon for a PRE switchover to be affected is when the active PRE has these issues:

- PRE module hangs
- Login to PRE console or Tenet to chassis fails
- Line cards unable to connect to active PRE module, hence crashing
- Cable modems drop offline
- Chassis reload required
- Reset of active PRE module requires to restore service

One of the reasons may be because the active PRE may not be able to release its control to the standby PRE, thus both the PRE modules behave as the primary PRE modules.

In Cisco IOS Release 12.2(33)SCE5, the PRE high-availability is enhanced to address the PRE switchover issue. The line card uses a link loop mechanism when both the PRE modules behave as primary PRE modules.

In this mechanism, the line card checks the packet sent from the active PRE module, and automatically does a switchover to the real active PRE. The link loop mechanism automatically connects to the real active PRE module based on the MAC address, thus increasing robustness. This mechanism activates before the IPC keepalive timeout mechanism between the route processor and the line card does.

Note The PRE high-availability enhancement applies to both SSO and RPR redundancy modes on the Cisco uBR10012 router. For information on configuring SSO, see *Stateful Switchover* document at: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html.

Note If you are using the Break key to collect information, ensure that it is performed within 36 seconds (36s Enhanced High System Availability. Redundancy (EHSA) keepalive timeout) to prevent a reset of the active PRE module.

Note In case there is hardware issue with the PRE module, do not reinsert the faulty PRE in the chassis. Inserting a faulty PRE (although a standby PRE) may cause the line card to switch to the faulty PRE causing the line card to crash and cable modems to go offline.

Using Redundant File Systems

Both the primary and standby PRE modules have active file systems that can be accessed to store and transfer files. Table below lists the available file systems, the filenames that you can use with CLI commands to access the file systems, and a short description of each.

Table 93: Cisco uBR10012 Router File Systems

File System	Filename for CLI Commands	Description
Bootflash Secondary bootflash	bootflash: sec-bootflash:	Stores image and dump files.
NVRAM Secondary NVRAM	nvram: sec-nvram:	Typically stores the system default configuration file and startup configuration file.
System	system:	Stores the running configuration and other system files.

File System	Filename for CLI Commands	Description
Disk 0 Disk 1 Slot 0 Slot 1 Secondary Disk 0 Secondary Disk 1 Secondary Slot 0 Secondary Slot 1	disk0: disk1: slot0: slot1: sec-disk0: sec-disk1: sec-slot0: sec-slot1:	Disk refers to an ATA Flash disk (48 or 128 MB). Slot refers to a Flash memory card (8, 16, or 20 MB).[58] 0 refers to the left slot on the PRE module. 1 refers to the right slot on the PRE module. The **sec** prefix refers to the Flash disk or card in the standby PRE module.
FTP TFTP RCP	ftp: tftp: rcp:	Protocols used to transfer files to and from remote devices.

58 Because of the small file system, the slot devices are not typically used on the Cisco uBR10012 router. The disk and sec-disk file systems are typically used instead.

You can use the Privileged EXEC commands **dir**, **del**, and **copy** to manage the contents of the file systems. You can also use the commands **mkdir** and **rmdir** to create and remove directories on Flash disks. You cannot use the commands **squeeze** and **undelete** on Flash disks.

Note For more information about using these file systems, see the *File Management* section in the Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide .

Console Port Usage After a PRE Module Switchover

When an active PRE module fails, and the standby PRE module becomes the active PRE module, you must use the console port on the new active PRE module to give CLI commands and display statistics for the router. If you have connected your PC or terminal to the console port on an active PRE module and a switchover occurs, you will no longer be able to access the console. The display will show the following error message:

```
Router#
Secondary console disabled
Router#
```

To access the console, move the PC or terminal's serial cable to the console port on the other PRE module, which is now acting as the active PRE module.

Reload PXF in the Standby PRE

Introduced in Cisco IOS Release 12.2(33)SCG2, the Reload PXF in the Standby PRE feature fixes most of the double-hit IRAM parity errors by reloading the Parallel Express Forwarding (PXF) in the standby PRE. The PXF can be reloaded periodically, or by a process based on timeout events, in the standby PRE. For the Reload PXF in the Standby PRE feature, both the PRE modules should run the same Cisco IOS Release 12.2(33)SCG2 or later releases.

When Toasters (PXF Network Processing ASICs) continue to run for more than six months, Instruction RAM (IRAM) of the Toasters could encounter parity error where some bits of the IRAM are inversed. If a packet that is injected into the Toasters reaches the affected memory bits, the PRE will crash. If the IRAM parity error occurs in the standby PRE, it could remain undetected for a long time. During this period, if the active PRE crashes, the standby PRE will also crash after switchover, leading to collapse of the Cisco CMTS. This is called a double-hit IRAM parity error.

Restrictions

- Services may be affected when switchover and periodic reload of the PXF occur at the same time. The probability of this coincidence can be calculated by the following formula: 10s/(30*6*24*3600) * A = 1/1555200 *A = A * 6.43e-7 A is the probability of IRAM parity error of toasters on one PRE board.
- Standby PRE crashes on Reload failure

For benefits of the Reload PXF in the Standby PRE feature, see the Reload PXF in the Standby PRE ensures Enhanced Stability, on page 889.

Benefits

PRE Modules are not a Single Point of Failure

The PRE module is no longer a single point of hardware failure. If a permanent hardware failure in the active PRE module occurs, the standby PRE module recovers the system, increasing the level of network service and reliability.

PRE Switchover Occurs Without Operator Intervention

The standby PRE module can become the active PRE module without the manual intervention of a system operator. This increases the recovery time and reduces the need for an instant response from the network administrators.

Protection Against Software Failure

The RPR feature does not operate as a hot standby system, in which the standby PRE module continually duplicates the state of the primary module. Instead, during a switchover, the standby PRE module begins operations from a known state, thereby protecting the system from the possible software or operations failures that might have affected the active PRE module.

Reload PXF in the Standby PRE ensures Enhanced Stability

The Reload PXF in the Standby PRE feature ensures enhanced stability of the Cisco uBR10012 router by providing the following enhancements:

- Prevent double-hit IRAM parity errors.
- Reloading the PXF in the standby PRE when a timeout event is generated.
- Prevents the standby PRE crash and subsequent crashing of the Cisco CMTS. If the current PRE is in standby mode, the Toasters and Cobalt3 are reset.
- Interval of periodic reload is set at six months.
- Reload is scheduled at 3 a.m. (0300) local time, which is estimated as low traffic time, for minimal performance impact.

Toaster IRAM Parity Improvement

Starting from Cisco IOS Release 12.2(33)SCJ1a, the system shuts down the TMC cores which has Toaster IRAM parity error, and keeps other cores running. It can avoid the PXF crush and PRE switch over.

This feature is enabled by default, it can be disabled using **no cable toaster-iram-recover** command, to re-enable it, use **cable toaster-iram-recover** command.

Restrictions

- TMC core shutting down can only initiate once. The second occurrence of the Toaster IRAM parity error will trigger PXF crush.
- PRE5 PXF consists of five Toasters, this solution is effective only on the first four, which are T0, T1, T2 and T3.

How to Configure Route Processor Redundancy

See the following sections for configuration tasks for the RPR feature.

Tip These procedures refer to primary and standby PRE modules. Under normal circumstances when the Cisco uBR10012 router starts up, the PRE module in slot A becomes the active PRE module. However, the PRE module in slot B could can also function as the active PRE module at any time. When using these procedures, be aware that the term active PRE module refers to whichever PRE module is active at the current time, not necessarily to a PRE module in a particular physical slot.

Note All CLI commands shown in these procedures must be given at the console for the active PRE module. You do not normally need to configure the standby PRE module because the RPR feature automatically synchronizes the configuration files between the primary and standby PRE modules. If you have connected your PC or terminal to the console port on a active PRE module and a switchover occurs, you will no longer be able to access the console, and the display will read “Secondary console disabled”. To access the console, move the PC or terminal's serial cable to the console port on the other PRE module, which is now acting as the active PRE module.

Configuring Route Processor Redundancy

The RPR feature on the Cisco uBR10012 router is automatically enabled when two PRE modules are installed in the Cisco uBR10012 chassis. By default the two PRE modules are also configured to automatically synchronize all critical system files.

Use the following procedure to change how the PRE modules synchronize the system files.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **main-cpu**
5. **auto-sync** *option*
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**main-cpu** **Example:** `Router(config-red)# main-cpu`	Enters the main CPU configuration mode. • This configures the active PRE module, not the standby PRE module.
Step 5	**auto-sync** *option* **Example:** `Router(config-r-mc)# auto-sync`*option*	Specifies the files to be synchronized. The *option* parameter can be one of the following: • **startup-config —**(Specifies that the PRE modules should synchronize the startup configuration files. • **config-register —**(Specifies synchronization of the configuration register values. • **bootvar —**(Specifies synchronization of the following boot variables: ◦ BOOT ◦ CONFIG_FILE ◦ BOOTLDR

	Command or Action	Purpose
		• **standard—**(Default) Specifies synchronization of all the system files.
Step 6	**end** **Example:** `Router(config-r-mc)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the current configuration as the default startup configuration.

Configuring Reload PXF in the Standby PRE

The Reload PXF in the Standby PRE feature on the Cisco uBR10012 router is disabled by default. Use the following procedure to enable the Reload PXF in the Standby PRE feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**periodic-rel-pxf enable** **Example:** `Router(config-red)# periodic-rel-pxf enable`	Enables the periodic PXF reload. **Note** This configuration enables the PXF to reload periodically in the standby PRE module.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-red)# end`	Returns to privileged EXEC mode.

Verifying Route Processor Redundancy

Use the following procedure to verify that RPR is configured on the Cisco uBR10012 router.

Step 1 Display the startup configuration and verify that the lines configuring redundancy appear:

Example:

```
Router# show startup-config

...
redundancy
 main-cpu
  auto-sync standard
...
```

Note If the **auto-sync** line contains anything other than **standard**, it indicates that only some of the required system files are being synchronized between the two PRE modules. Verify that this is the desired configuration, and if necessary, use the procedure given in the Configuring Route Processor Redundancy, on page 890 to reconfigure the router for **auto-sync standard** operation.

Step 2 Display the current RPR state using the **show redundancy** command. The Active PRE typically is shown in slot A:

Example:

```
Router# show redundancy

 PRE A (This PRE)    : Primary
 PRE B               : Secondary

 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED

 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
```

If a switchover has occurred, the **show redundancy** command will produce a display similar to the following, showing that the Active PRE has changed slots (in this case, moving from slot A to slot B):

Example:

```
Router# show redundancy

 PRE A               : Secondary
 PRE B (This PRE)    : Primary
```

```
 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED

 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
Router#
```

If the standby PRE module is not installed or is not operational, the **show redundancy** command will produce a display similar to the following:

Example:

```
Router# show redundancy

 PRE A (This PRE)   : Primary
 PRE B              : Secondary
 Redundancy state is REDUNDANCY_PEERSECONDARY_NONOPERATIONAL
 Secondary PRE information....
 Secondary PRE is not up
```

What to Do Next

Note The **show redundancy** command shows whether the PRE A slot or PRE B slot contains the active (**Primary**) PRE module. The other PRE slot will always be marked as **Secondary**, even if a second PRE module is not installed.

Forcing Switchover

To manually force a switchover, so that the standby PRE module becomes active, use the **redundancy force-failover main-cpu** command in Privileged EXEC mode. Manually forcing a switchover is useful in the following situations:

- You need to remove, replace, or upgrade the currently active PRE module.
- A previous switchover has activated the standby PRE module and you now want to restore the previously active PRE module.

Tip Simply removing the active PRE module would also trigger a switchover, but using the **redundancy force-failover main-cpu** command does not generate a hardware alarm.

The following procedure shows the procedure to force a switchover from the primary to the standby PRE module.

Step 1 Use the **redundancy force-failover main-cpu** command to force the switchover:

Example:

```
Router# redundancy force-failover main-cpu
Proceed with switchover to standby PRE? [confirm]

 00:38:09: %SYS-5-RELOAD: Reload requested
 System Bootstrap, Version 12.0(9r)SL1, RELEASE SOFTWARE (fc1)
 Copyright (c) 2000 by cisco Systems, Inc.

 Reset Reason Register = RESET_REASON_RESET_REG (0x74)
 C10000 platform with 524288 Kbytes of main memory
...
```

Step 2 After the switchover has occurred, the standby PRE module becomes the active PRE module, and the previous active PRE module is put into the ROM monitor mode. To enable that module to become the new standby PRE module, use the **hw-module sec-cpu reset** command so that the module will initialize and begin monitoring the health of the active PRE module:

Example:

```
Router# hw-module sec-cpu reset

Router#
11:55:09: %REDUNDANCY-5-PEER_MONITOR_EVENT: Primary detected a secondary crash
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
```

Verifying the PRE Switchover

Use the following procedure to verify that the switchover has occurred:

Step 1 Check that the Status LED on the new active, active PRE module is lighted with a steady green to indicate that it has initialized and is acting as the active PRE module. The alphanumeric display should also show a series of dashes to indicate that the PRE module is running without problems.

Step 2 Check that the Status LED on the new standby PRE module is OFF and that the alphanumeric display shows the message **IOS STBY** to indicate that the module is now acting as the standby PRE module.

Note After a failure, the non-active PRE module will either reload the Cisco IOS software image or enter ROM monitor mode, depending on the setting of its configuration register. If it loads the Cisco IOS software, it will automatically begin functioning as a standby PRE module. If it enters ROM monitor mode, it will become the standby PRE module only if it is reloaded using the **hw-module sec-cpu reset** command.

Step 3 To verify that a switchover has occurred, use the **show redundancy** command. Assuming that the original PRE module had been in slot A, and that the standby PRE module is in slot B, the **show redundancy** command would display the following:

Example:

```
Router# show redundancy

 PRE A               : Secondary
 PRE B (This PRE)    : Primary

 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED
```

```
 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
Router#
```

Verifying Reload PXF in the Standby PRE

To verify that the Reload PXF in the Standby PRE feature is enabled, use the **show running-config | include periodic** command in privileged EXEC mode.

```
Router# show running-config | include periodic

periodic-rel-pxf enable

Router#
```

Upgrading Cisco IOS Software on the PRE Modules

This section describes how to upgrade the software on redundant PRE modules in the Cisco uBR10012 router. This procedure requires that all PRE system files be synchronized, using the default synchronization setting (**auto-sync standard**).

Note The following CLI and ROM monitor commands must be given through the console port on the active PRE module. Although the CLI commands can be given through a Telnet connection to the active PRE module, this is not recommended because the ROM monitor commands require a connection to the active PRE module's serial console port.

Step 1 If not already done, copy the new Cisco IOS software image from the TFTP server to the Flash disk in slot 0 of the active PRE module:

Example:

```
Router# copy tftp disk0:
Address or name of remote host [ ]? 192.168.100.10

Source filename [ ]? ubr10k-k8p6-mz.122-4.XF

Source filename [ubr10k-k8p6-mz.122-4.XF]?
Accessing tftp://192.168.100.10/ubr10k-k8p6-mz.122-4.XF
Loading ubr10k-k8p6-mz.122-4.XF from
192.168.100.10 (via FastEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
[OK - 5717476/11433984 bytes]
5717476 bytes copied in 250.840 secs (22869 bytes/sec)
Router#
```

Step 2 Copy the same image to the Flash disk in slot 0 of the standby PRE module:

Example:

```
Router# copy disk0:ubr10k-k8p6-mz.122-4.XF sec-disk0:
```

Step 3 Configure the system to use the new software image. In the following example, the Cisco uBR10012 router will use the software image named **ubr10k-k8p6-mz.122-4.XF** on the Flash disk in slot 0 of the active PRE module:

Example:

```
Router(config)# boot system flash disk0:ubr10k-k8p6-mz.122-4.XF
```

Step 4 If necessary, save the running configuration to the startup configuration:

Example:

```
Router# copy running-config startup-config
```

Step 5 Reset the standby PRE module so that it reboots and uses the new image.:

Example:

```
Router# hw-module sec-cpu reset
```

Step 6 Force a cutover to the standby PRE module, which forces the active PRE module to reboot and use the new image:

Example:

```
Router# redundancy force-failover main-cpu
```

Verifying the Software Upgrade

Use the following procedure to verify that the Cisco uBR10012 router is running the new upgraded Cisco IOS software image.

Step 1 Connect a PC or terminal to the console port of the active PRE module and give the **show version** command, which displays the version number and image name of the currently running software image:

Example:

```
Router# show version

 Cisco Internetwork Operating System Software
```

Example:

```
 Copyright (c) 1986-2001 by cisco Systems, Inc.
 Compiled Wed 1-Nov-01 22:36 by abc
 Image text-base: 0x600089C0, data-base: 0x61330000

 ROM: System Bootstrap, Version 12.0(9r)SL2, RELEASE SOFTWARE (fc1)
 BOOTLDR: 10000 Software (C10K-EBOOT-M), Version 12.0(16.6)ST2, RELEASE SOFTWARE
 Router uptime is 0 hours, 4 minutes
 System returned to ROM by power-on
```

Example:

Step 2 Connect a PC or terminal to the console port of the standby PRE module and give the **show version** command. This command should display the same name and version information as shown on the active PRE module.

Changing the System Boot Behavior

This section describes how to change the Cisco IOS software configuration register to modify how the system behaviors at power-on or reboot. The software configuration register is a 16-bit register in NVRAM that controls the following boot functions:

- Specifies the source of the Cisco IOS software image to be loaded
- Specifies whether the Cisco IOS software should ignore the contents of the saved configuration file in NVRAM memory
- Enables or disables the use of the Break function

Use the following procedure to change the software configuration register settings:

Step 1 Enter global configuration mode and use the **config-register** command to set the contents of the software configuration register to a new value. You must specify the new value as a 16-bit hexadecimal bitmask, using the values shown in the Table below.

Table 94: Definition of Bits in the Software Configuration Register

Bit No.	Hex Value	Meaning/Function
00 to 03	0x0000 to 0x000F	Defines the source of a default Cisco IOS software image required to run the router: • 00—On powerup, the system remains at the ROM monitor prompt (rommon>), awaiting a user command to boot the system manually by means of the rommon **boot** command. • 01—On powerup, the system automatically boots the first system image found in the Flash memory single inline memory module (SIMM) on the PRE. • 02 to 0F—On powerup, the system automatically boots from a default Cisco IOS software image stored on a TFTP server in the network. For this setting, the Fast Ethernet port on the PRE must be configured and operational. This setting also enables boot system commands that override the default filename.
06	0x0040	Causes system software to ignore the contents of the NVRAM configuration file.
07	0x0080	Enables the original equipment manufacturer (OEM) bit.
08	0x0100	Disables the Break function after 30 seconds.
09	0x0200	Not used.
10	0x0400	Specifies that broadcast packets are based on the 0.0.0.0 IP address.
11 and 12	0x0800 to 0x1000	Defines the console baud rate (the default setting is 9600 baud).

Bit No.	Hex Value	Meaning/Function
13	0x2000	Boots an image from the Flash memory.
14	0x4000	Specifies that broadcast packets use the subnet broadcast address.
15	0x8000	Enables diagnostic messages and ignores the contents of the NVRAM configuration file.

For example, to configure the router to boot to the ROM monitor prompt, set the configuration register to **0x2100** with the following commands:

Example:

```
Router#
config t

Router(config)#
config-register 0x2100

Router(config)#
```

Tip The typical bitmask for normal use is 0x2102, which specifies that the router loads the Cisco IOS software from the Flash memory and boots to the Cisco IOS CLI prompt. The Break key is enabled for only 30 seconds, so that the user can break to the ROM monitor prompt if desired.

Step 2 Exit the global configuration mode by entering the **exit** command.

Example:

```
Router(config)# exit

Router#
```

Step 3 Display the new software configuration register setting using the **show version** command. The last line shows the settings of the configuration register:

Example:

```
Router#
show version

Cisco Internetwork Operating System Software
 IOS (tm) 10000 Software (UBR10K-K8P6-MZ), Released Version 12.2(4)XF
 Copyright (c) 1986-2001 by cisco Systems, Inc.
...
```

Example:

Note When you change the configuration register, the **show version** command shows both the current value of the register, as well as the value that will be used on the next reboot or reload.

Step 4 Save the configuration file to preserve the new software configuration register settings.

Example:

```
Router# copy running-config startup-config
```

Step 5 The changes to the software configuration register will take effect the next time the router is rebooted or restarted. To manually reboot the router, use the **reload** command:

Example:

```
Router# reload
System configuration has been modified. Save? [yes/no]: yes
Proceed with reload? [confirm]
```

What to Do Next

Note For detailed information about setting and using the configuration register, see the *Rebooting* chapter in the *File Management* manual, which is part of the *Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*.

Moving a Configuration File to the Flash Disk

This section describes how to copy a configuration file to a Flash disk and configure the Cisco uBR10012 router so that it loads the configuration file from the Flash disk. This typically is necessary when the configuration file is approaching the 512KB maximum size that is allowed for configuration files that are stored in NVRAM.

Use the following procedure to copy and run the startup configuration off a Flash disk.

Step 1 The configuration file must fit within one complete buffer on the Flash disk. The default buffer size is 512 KB, so if the configuration file is larger than this, or if you ever expect the file to be larger than this, you will need to change the buffer size. To do so, enter global configuration mode and change the buffer size with the **boot buffersize** command. The following shows the buffer being changed to 1 MB in size:

Example:

```
Router# configure terminal
Router(config)# boot buffersize 1024000
Router(config)# exit
Router#
```

Step 2 Copy the configuration file to the Flash disks in both PRE modules. The following example assumes the configuration file is still small enough to exist in NVRAM and is being copied to the first Flash disk in each PRE module:

Example:

```
Router# copy nvram:ubr10012-config disk0:ubr10012-config
Router# copy nvram:ubr10012-config sec-disk0:ubr10012-config
Router#
```

If the configuration file is currently on a TFTP server, the following commands copy the file to the first Flash disk in each PRE module:

Example:

```
Router# copy tftp://192.168.100.10/router-config disk0:ubr10012-config
Router# copy disk0:ubr10012-config sec-disk0:ubr10012-config
Router#
```

Step 3 Specify the new location of the configuration file by setting the CONFIG_FILE boot variable with the **boot config** command in global configuration mode. For example, the following specifies

Example:

```
Router# config t
Router(config)# boot config disk0:ubr10012-config
Router(config)# exit
Router#
```

Step 4 When you have finished changing the running-configuration, save the new configuration:

Example:

```
Router# copy running-config startup-config
```

What to Do Next

When the Cisco uBR10012 router next restarts or reboots, the router will use the configuration file on the first Flash disk in the active PRE module.

Verifying the Configuration File Setting

To verify that the Cisco uBR10012 router is configured to use the startup configuration file on the Flash disk, use the following procedure:

Step 1 Display the directory of the Flash disk in the active PRE module:

Example:

```
Router# dir disk0:
```

```
Directory of disk0:/
    1  -rw-    10705784   May 30 2001 20:12:46  ubr10k-k8p6-mz.122-4.XF
    2  -rw-      484772   Jun 20 2001 19:12:56  ubr10012-config
128094208 bytes total (116903652 bytes free)
Router#
```

Step 2 Display the directory of the Flash disk in the standby PRE module:

Example:

```
Router# dir sec-disk0:

Directory of sec-disk0:/
    1  -rw-    10705784   May 30 2001 20:12:46  ubr10k-k8p6-mz.122-4.XF
    2  -rw-      484772   Jun 20 2001 19:12:56  ubr10012-config
128094208 bytes total (116903652 bytes free)
Router#
```

Note The contents of the Flash disk in the standby PRE module should be similar or identical to the contents of the Flash disk in the active PRE module.

Step 3 Display the setting of the CONFIG_FILE boot variable using the **show bootvar** command:

Example:

```
Router# show bootvar

BOOT variable =
CONFIG_FILE = disk0:ubr10012-config
BOOTLDR variable =
Configuration register is 0x2102
```

Configuration Examples for Route Processor Redundancy

The following example shows the relevant portion of the Cisco IOS configuration file for the default configuration for the RPR feature, which should be used for most applications:

```
redundancy
  main-cpu
   auto-sync standard
```

The following example shows the relevant portion of the Cisco IOS configuration file for the configuration that could be used when the two PRE modules are running different Cisco IOS software images and require different configuration files:

```
redundancy
  main-cpu
   no auto-sync startup-config
   auto-sync config-register
   auto-sync bootvar
```

Additional References

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
CMTS Hardware Installation Guide	Cisco uBR10012 Series Hardware Installation Guide
CMTS Software Installation Guide	Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC
CMTS Troubleshooting Guide	Cisco uBR10012 Series Troubleshooting Guide
Route Processor Performance Routing Engines	Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module
Route Processor Redundancy Plus for Cisco CMTS	Route Processor Redundancy Plus for the Cisco uBR10012 Universal Broadband Router
Stateful Switchover	Stateful Switchover
In Service Software Upgrade	Cisco IOS In Service Software Upgrade

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Route Processor Redundancy

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 95: Feature Information for Route Processor Redundancy

Feature Name	Releases	Feature Information
Route Processor Redundancy	12.2(4)XF	This feature was introduced on the Cisco uBR10012 universal broadband router.
	12.2(4)BC1	Support for this feature was added to Cisco IOS Release 12.2 BC for the Cisco uBR10012 universal broadband router.

Feature Name	Releases	Feature Information
	12.2(11)CY, 12.2(11)BC3	Support for the PRE module was removed. Only the PRE1 module can be used with the Cisco uBR10012 router**.**
	12.2(33)SCA	This feature was intergrated in Cisco IOS Release 12.2(33)SCA for Cisco uBR10012 router.
	12.2(33)SCE5	PRE high availability was enhanced. A link loop mechanism was added to the PRE switchover.
Reload PXF in the Standby PRE	12.2(33)SCG2	This feature is introduced on Cisco uBR10012 universal broadband router. The following were introduced or modified: **periodic-rel-pxf enable**

CHAPTER 33

Route Processor Redundancy Plus for the Cisco uBR10012 Broadband Router

First Published: February 14, 2008

This document describes the Route Processor Redundancy Plus (RPR+) feature on the Cisco uBR10012 universal broadband router. RPR+ and DOCSIS Stateful Switchover (DSSO) support in Cisco IOS® Software for fast route processor failover without DOCSIS line card reboot.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

With RPR+ and DOCSIS SSO, the Cisco uBR10012 can rapidly fail over from the active route processor to the standby processor without the reloading of the cable line cards. However, even though the cable line cards are not reset, the new active route processor needs to perform certain recovery procedures in order for cable line card traffic-flow to resume. A Cisco implementation provides priority-recovery procedures for those modems carrying voice, providing more rapid recovery of voice services.

Note From Cisco IOS release 12.2SC onwards, NSF and SSO is recommended and supported on the Cisco uBR10012 router. For SSO configuration details, see the "Configuring SSO" section in the Stateful Switchover guide at the following link: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/sso26s.html#wp1338159

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Route Processor Plus Redundancy

- You must have the same image on both the active and standby RPs to support RPR+. If one or more RPs does not have an RPR+ image, the router reverts to RPR mode on both RPs.
- Two PRE1 or PRE2 modules must be installed in the Cisco uBR10012 chassis. The order number for the PRE1 module is UBR10-PRE1. You cannot mix PRE modules with PRE1 or PRE2 modules in the same chassis.

Note The PRE module no longer ships with the Cisco uBR10012 chassis.

- For full redundancy, the Fast Ethernet port on the standby RP must have its own connection to the network. The console port on the standby RP must also be connected to a terminal, either by connecting it to a second terminal or by using a terminal server or other device to connect it to the same terminal used by the PRE1 or PRE2 module.
- Both PRE1 or PRE2 modules must be configured with the same amount of onboard SDRAM. A standby RP cannot come online as the active RP if the standby RP has a smaller amount of SDRAM than the active RP.

Restrictions for Route Processor Plus Redundancy

ARP Filtering Statistics

The Cisco uBR10012 router maintains ARP filtering statistics on the Performance Routing Engine (PRE) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in RPR+ Redundancy, these ARP filtering statistics are reset to zero.

For additional 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

Command-line Interface Synchronization and SNMP

Command-line interface (CLI) configuration commands are synchronized only with the standby Performance Routing Engine (PRE) module. Simple Network Management Protocol (SNMP) persistence is not supported through a PRE1 or PRE2 switchover. Any configuration that is done with SNMP commands is not synchronized with the standby PRE module.

Console Port Usage After a PRE1 or PRE2 Module Switchover

When an active RP fails, and the standby RP becomes the active RP, you must use the console port on the new active RP to give command-line interface (CLI) commands and display statistics for the system. If you have connected your PC or terminal to the console port on an active RP and a switchover occurs, you no longer are able to access the console and the display shows "Standby console disabled."

To access the console, move the PC or terminal's serial cable to the console port on the other PRE1 or PRE2 module, which is now acting as the active RP.

Encrypted Multicast

Encrypted multicast is not supported during a line card switchover nor during a PRE1 or PRE2 switchover.

External Management Stations

External management stations lose connectivity with the cable modem termination system (CMTS) during PRE1 or PRE2 switchover. Stations must reestablish connectivity after the switchover between PRE1 or PRE2 modules is complete.

Flap Detection on WAN Interfaces During Switchover

Neighboring routers detect flapping on WAN interfaces during a switchover. The neighboring routers reconverge after the switchover is complete.

Note Cable interfaces do not flap during a switchover. Service may be temporarily suspended for approximately 30 seconds during a switchover and reinitialization, but service to cable interfaces does not stop.

Link States Reinitialized After Switchover

The synchronization of link states is not maintained between the active and standby RP. Link states are reinitialized after switchover

MIB Variables Reinitialized After Switchover

All MIB variables will be re-initialized following a switchover.

Telnet Sessions Disconnected During Switchover

A switchover automatically disconnects any Telnet sessions on the active (failed) RP.

Information About Route Processor Plus Redundancy

When two route processors (RPs) are installed in a Cisco uBR10012 router chassis, one RP acts as the active RP, and the other acts as a backup, or standby, RP. If the active RP fails, or is removed from the system, the

standby RP detects the failure and initiates a switchover. During a switchover, the standby RP assumes control of the router, connects with the network interfaces, and activates the local network management interface and system console.

Using the RPR+ feature, the standby RP is fully initialized and configured. This allows RPR+ to dramatically shorten the switchover time if the active RP fails, or if a manual switchover is performed. Because both the startup configuration and running configuration are continually synchronized from the active to the standby RP, line cards are not reset during a switchover. The interfaces remain up during this transfer, so neighboring routers do not detect a link flap (that is, the link does not go down and back up).

Each RP contains all the resources required to operate the router, such as bootflash memory, Flash disks, Ethernet ports, and console port. In the default operation, the secondary RP also synchronizes the major systems files, such as the Cisco IOS startup configuration file, so that during a switchover, the secondary RP can duplicate the active RP's configuration. This process also resets the cable and network uplink interfaces.

This section describes the switchover process with RPR+, including synchronization between the active and standby RPs, and includes the following topics:

Benefits

DOCSIS Stateful Switchover (DSSO)

DOCSIS stateful switchover (DSSO) increases service uptime by instantaneously switching over between dual route processors should one processor fail. Switchover takes place without resetting or reloading line cards or affecting related subsystems or processes. The advantage of DOCSIS Stateful Switchover (DSSO) (with RPR+) is that a switchover between the primary and standby RP will not require the cable interfaces to be reset, nor do the modems reregister or go offline. Furthermore, the cable modems retain their service IDs (SIDs) through the switchover.

Standard RPR

In standard RPR, the system implemented Extended High System Availability (EHSA) redundancy, wherein the standby RP suspended its initialization midway through the startup process. To complete the initialization during a switchover, all line cards were reset and the switch fabric was reinitialized. Because initialization of the standby RP was suspended before configuration was parsed, chassis discovery and startup configuration parsing were conducted during the switchover.

Improved Switchover Time with RPR+

RPR+ provides a faster switchover by fully initializing and fully configuring the standby RP. The configuration data on the standby RP is fully synchronized with the active RP. With RPR+, the communication with line cards is reinitialized, but the line cards are not reset.

Supported Cable Interface Line Cards and Interface Modules

Beginning with Cisco IOS Release 12.2(11)BC3, the Cisco uBR10012 router supports the following cable interface line cards and interface modules with RPR+ and PRE1 or PRE2 modules:

- Cisco uBR10-LCP2-MC16C/MC16E/MC16S Line Card
- Cisco uBR10-LCP2-MC28C/B Line Card
- Cisco uBR10-MC5X20S Cable Interface Line Card
- Cisco uBR10-SRP-OC12SML/SMI DPT Adapter Card

- Cisco uBR10012 OC-48 DPT/POS Interface Module

Terminology Changes with Cisco IOS Release 12.2(11)BC3

In Cisco IOS Release 12.2(11)BC3 and later, the following High Availability terms for the Cisco uBR10012 universal broadband router have been changed:

Old Term	New Term
Failover	Switchover
N+1 Redundancy	1:n Redundancy
Primary RP	Active RP
Secondary RP	Standby RP

Synchronization

To achieve the benefits of RPR+, the chassis and slot configuration information is synchronized from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. This synchronization occurs in two separate phases:

1. When a standby RP first comes online, the configuration information is synchronized in bulk from the active RP to the standby RP.
2. When configuration changes occur, an incremental synchronization from the active RP to the standby RP is conducted. Incremental synchronizations contain either the modifications to the shelf configuration or the trigger that caused the modification.

Synchronization During Initialization

When a system with RPR+ is initialized, the active RP performs a chassis discovery (discovery of the number and type of line cards and fabric cards in the system) and parses the startup configuration file.

The active RP then synchronizes this data to the standby RP and instructs the standby RP to complete its initialization. This method ensures that both RPs contain the same configuration information.

Note Even though the standby RP is fully initialized, it interacts only with the active RP to receive incremental changes to the configuration files as they occur. CLI commands on the standby RP are not supported.

Synchronization of Startup Configuration

The startup configuration is a text file stored in the RP's NVRAM. During system startup, the startup configuration file is copied from the active RP to the standby RP. Any existing startup configuration file on the standby RP is overwritten.

The startup configuration file is also synchronized whenever you perform the following operations:

- CLI command: copy system:running-config nvram:startup-config
- CLI command: copy running-config startup-config
- CLI command: write memory
- CLI command: copy filename nvram:startup-config
- SNMP SET of MIB variable ccCopyEntry in CISCO_CONFIG_COPY MIB
- System Configuration Saved on reload command.
- System Configuration Saved on redundancy force-failover command.

Note Synchronization of the startup configuration file is enabled by default in RPR+ mode. Because this is necessary for RPR+ functionality, the command [no] auto-sync startup-config is not available in RPR+ mode. This command is available only in standard RPR mode. For additional information on the use of [no] auto-sync startup-config with standard RPR, see the Route Processor Redundancy for the Cisco uBR10012 Universal Broadband Router .

Incremental Synchronization of the Running Configuration

When both RPs are fully initialized, any further changes to the running configuration are synchronized to the standby RP as they occur.

CLI commands

CLI changes to the running configuration are synchronized from the active RP to the standby RP. In effect, the CLI command is run on both the active and the standby RP.

SNMP SET Commands

Configuration changes caused by an SNMP SET are also synchronized on a case-by-case basis. Currently only two SNMP configuration SETs are supported on the Cisco uBR10012 router:

- shut/no-shut (of an interface)
- link up/down trap enable/disable

Changes to Chassis State

- Any changes to the chassis state because of line card insertion or removal are synchronized over to the standby RP.
- Changes to the chassis state because of switch card insertion or removal, or from configuration changes to the alarm or power supply cards, are not synchronized to the standby RP. The standby learns these configuration changes using a discovery and reconciliation process during a switchover.
- Information regarding line card states is not synced. Line cards that are not on line at the time of a switchover (that is, any cards not running the Cisco IOS software and not communicating with the active RP) are reset and reloaded during a switchover. This process does not add downtime.

The RPR+ Switchover Process

A switchover occurs when the standby RP takes over responsibilities from the active RP. The switchover can occur automatically if the standby RP has determined that the active RP has failed, or an operator can initiate a manual switchover whenever desired.

A switchover triggers the following events:

1. If this is a manual switchover, the active RP verifies that the standby RP is present and is running Cisco IOS software that supports the RPR feature. If so, it instructs the standby RP to begin switchover procedures, and the active RP either attempts to reload its configured Cisco IOS software image or enters ROM monitor mode, depending on the setting of its configuration register.
2. The standby RP completes its initialization procedures, which includes completely loading the Cisco IOS software, verifying the physical components of the Cisco uBR10012 chassis, and parsing the startup configuration file. The standby RP is configured identically to the previous active RP, including the IP address for its onboard Fast Ethernet management interface.
3. The standby RP assumes responsibility as the active RP and brings the Cisco uBR10012 chassis into a known state, which includes resetting all installed and enabled line cards and respective interfaces.

Note Resetting the Gigabit Ethernet and OC-12 Packet Over SONET (POS) line cards will interrupt traffic for approximately 30 seconds. The cable interface is not reset, and in support of DOCSIS requirements, the cable modems do not go offline.

Note Depending on the network configuration and on the configuration of the Ethernet/Fast Ethernet interfaces, the network could take between 3 to 25 seconds after an RPR+ switchover before all end-to-end connections are fully restored. During that time it is possible that some packets might be dropped.

1. The new active RP begins normal systems operations, including passing traffic.

Note Depending on the setting of the PRE1 or PRE2 module's configuration register, it either reloads the Cisco IOS software or is left in the ROM monitor state. If the PRE1 or PRE2 module is in the ROM monitor state, it does not begin functioning as a standby RP until it is reloaded with the hw-module sec-cpu reset command.

Note The backup PRE1 or PRE2 module starts forwarding traffic immediately to cable modems, presuming that the interfaces are up, and that all the FIB, adjacency, service flow, classifiers, and Virtual Traffic Management System (VTMS) queue information are correctly configured.

Redundant File Systems

Both the active and standby RPs have active file systems that can be accessed to store and transfer files. Table 1 lists the available file systems, the filenames that you can use with CLI commands to access the file systems, and a short description of each.

Table 96: Cisco uBR10012 Router File Systems

File System	Filename for CLI Commands	Description
Bootflash Secondary bootflash	bootflash: sec-bootflash:	Stores image and dump files.
NVRAM Secondary NVRAM	nvram: sec-nvram:	Typically stores the system default configuration file and startup configuration file.
System	system:	Stores the running configuration and other system files.
Disk 0 Disk 1 Slot 0 Slot 1 Secondary Disk 0 Secondary Disk 1 Secondary Slot 0 Secondary Slot 1	disk0: disk1: slot0: slot1: sec-disk0: sec-disk1: sec-slot0: sec-slot1:	Disk refers to an ATA Flash disk (48 or 128 MB). Slot refers to a Flash memory card (8, 16, or 20 MB).[59] 0 refers to the left slot on the PRE1 or PRE2 module. 1 refers to the right slot on the PRE1 or PRE2 module. The sec prefix refers to the Flash disk or card in the standby RP.
FTP TFTP RCP	ftp: tftp: rcp:	Protocols used to transfer files to and from remote devices.

59 Because of the small file system, the slot devices are not typically used on the Cisco uBR10012 router. The disk and sec-disk file systems are typically used instead.

You can use the privileged EXEC commands dir, del, and copy to manage the contents of the file systems. You can also use the commands mkdir and rmdir to create and remove directories on Flash disks. You cannot use the commands squeeze and undelete on Flash disks.

Note For more information about using these file systems, see the "File Management" manual in the Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide.

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+) for the Cisco uBR10012 router, with Active and Standby Performance Routing Engines (PREs)
- HCCP N+1 Redundancy, with Working and Protect cable interface line cards

For further information about DSX messages and Payload Header Suppression (PHS) information on the Cisco CMTS, refer to these documents, and additional DOCSIS PHS information:

- *Cable DOCSIS 1.1 FAQs* , Cisco TAC Document 12182

http://www.cisco.com/en/US/tech/tk86/tk168/technologies_q_and_a_item09186a0080174789.shtml

- DOCSIS 1.1 for the Cisco CMTS

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.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/12_2sc/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/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html

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

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun.html

How to Configure, Verify, and Troubleshoot Route Processor Plus Redundancy

This section provides the following procedures to configure and verify RPR+ and high availability on the Cisco uBR10012 router.

Configuring RPR+ on the Cisco uBR10012 Universal Broadband Router

The default redundancy mode in the Cisco uBR10012 router is standard Route Processor Redundancy (RPR). Perform the steps below to enable RPR+ on the Cisco uBR10012 router.

Before You Begin

To enable RPR+, both route processors must be running the same version of Cisco IOS software.

Note If necessary, refer to the "Upgrading Cisco IOS Software Images" section on page 14 to change the image on the Cisco uBR10012 router. Reload is required.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**main-cpu** **Example:** `Router(config)# main-cpu`	Enters the main CPU configuration mode. (This configures the active RP, not the standby RP.) Refer to **main-cpu** command, for additional command syntax information.
Step 4	auto-sync option **Example:** `Router(config-r-mc)# auto-sync standard`	Specifies the files to be synchronized. Refer to **auto-sync** command, for additional command syntax information. **Note** Cisco strongly recommends that you use the auto-sync standard command to ensure that all system files remain synchronized between the two PRE1 or PRE2 modules.
Step 5	**no auto-sync** *option* **Example:** `Router(config-r-mc)# no auto-sync standard`	(Optional) Specifies that one or more files should not be synchronized. Option can be any of the values specified previously. **Note** The **no auto-sync** command is not typically used in production plants.
Step 6	**CTRL-Z** **Example:** `Router(config-r-mc)# CTRL-Z`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the current configuration as the default startup configuration.

Verifying RPR+ Configuration

Perform the steps below to verify that RPR+ is configured on the Cisco uBR10012 router:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show startup-config** **Example:** `Router# show startup-config` `...` `redundancy` `main-cpu` `auto-sync standard` `...`	Displays the startup configuration and verify that the lines configuring redundancy appear. **Note** If the auto-sync line contains anything other than standard, it indicates that only some of the required system files are being synchronized between the two PRE1 or PRE2 modules. Verify that this is the desired configuration. If necessary, refer to the Configuring RPR+ on the Cisco uBR10012 Universal Broadband Router, on page 915 to reconfigure the router for auto-sync standard operation.
Step 3	**show redundancy** **Example:** `Router# show redundancy` `PRE1 A (This PRE1) : Primary` `PRE1 B : Secondary` `...`	Displays the current RPR state. The active RP typically is shown in slot A.

If a switchover has occurred, the show redundancy command displays information similar to the following, showing that the active RP has changed slots (in this case, moving from slot A to slot B):

```
Router# show redundancy
PRE1 A : Secondary
PRE1 B (This PRE1) : Primary
Redundancy state is REDUNDANCY_PEERSECONDARY_INITED
Secondary RP information....
Secondary is up.
Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
Secondary CONFIG_FILE variable =
Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
Secondary Configuration register is 0x2
Router#
```

If the standby RP is not installed or is not operational, the show redundancy command displays information similar to the following:

```
Router# show redundancy
PRE1 A (This PRE1) : Primary
PRE1 B : Secondary
Redundancy state is REDUNDANCY_PEERSECONDARY_NONOPERATIONAL
Secondary RP information....
Secondary RP is not up
```

Note The show redundancy command shows whether the PRE1 A slot or PRE1 B slot contains the active (Primary) PRE1 module. The other PRE1 slot will always be marked as Secondary, even if a second PRE1 module is not installed.

Upgrading Cisco IOS Software Images

RPR+ is enabled by default with the Cisco IOS Release 12.2(11)BC3 and later releases. Use this set of procedures when you need to upgrade your Cisco IOS to a release that supports RPR+ on the Cisco uBR10012 router.

Cisco IOS software upgrade involves these three procedures:

Prerequisites

Note You are required to have the same image on both the active and standby RPs to support RPR+. If one or more RPs does not have an RPR+ image, the router reverts to RPR mode on both RPs.

Creating Additional Disk Space (Optional)

(Optional) To create additional disk space in preparation for the RPR+ image, issue the following commands from global configuration mode on the active and standby RPs (where slot is the RP slot number and filename is the RPR+ image file name).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • delete slot 0:filename • delete sec-slot 0:filename **Example:** `Router(config)# delete slot 0:ubr10k-p6-mz` or `Router(config)# delete sec-slot 0:ubr10k-p6-mz`	Deletes an old file from the active or standby RP to make room for the new file.
Step 2	squeeze flash: **Example:** `Router(config)# squeeze flash:`	Permanently deletes all files marked "delete" on a Flash memory device, recovering space on the device.

Copying the Cisco IOS Image

To copy the Cisco IOS image from a TFTP server, and to set the boot variable on the active RP, issue the following commands in global configuration mode (where filename is the RPR+ image fil name).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • copy tftp://tftp-server/filename bootflash:filename • • copy tftp://tftp-server/filename sec-bootflash:filename **Example:** `Router# copy tftp://tftp-server/ubr10k-p6-mz bootflash:ubr10k-p6-mz` `or` `Router# copy tftp://tftp-server/ubr10k-p6-mz sec-bootflash:ubr10k-p6-mz`	Copies the Cisco IOS image from a TFTP server to the bootflash of the active or standby RP. This command allows you to change software images without requiring access to the TFTP monitor mode. The image you download is made available to the Cisco uBR10012 router on the next reload (reboot).
Step 2	boot system bootflash:filename **Example:** `Router# boot system bootflash:ubr10k-p6-mz`	Sets the BOOT environment variable. This variable specifies the location and name of the system image file to use when automatically booting the system.
Step 3	write memory **Example:** `Router# write memory`	Saves the configuration.
Step 4	**show bootvar** **Example:** `Router# show bootvar`	Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.

Resetting a PRE1 or PRE2 Module or Line Card After Upgrade

To reset a particular route processor (RP) or a particular line card, use the hw-module reset command in privileged EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**hhw-module sec-cpu reset** **Example:** `Router# hw-module sec-cpu reset`	Resets the specified RP or line card slot. **Note** Refer to **hw-module reset command** for additional command syntax information.

Reloading Cisco IOS (Restarting the System)

To reload the operating system, use the reload command in privileged EXEC mode.

Note This reload is required if you are reloading an RPR+ image, but optional otherwise. The reload command restarts the entire system, including both the active and standby RPs.

SUMMARY STEPS

1. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**reload** **Example:** `Router# reload`	Reloads the operating system and restarts the router.

What to Do Next

Note If you are upgrading from a Cisco IOS image previously configured with RPR+ to a newer image with RPR+, the procedure is now complete. When the new active RP comes up, it will automatically configure RPR+ from the configuration information in the startup configuration (synchronized from the old active RP).

Performing a Manual Route Processor Switchover

For testing or maintenance, you may need to perform a manual switchover in which your standby RP becomes your active RP. Perform the following steps to force a manual switchover between RPs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show cable modem** **Example:** `Router> show cable modem`	Displays information for the registered and unregistered cable modems supported by the active RP. The output from this command provides information that confirms successful switchover in pending steps.
Step 2	**redundancy force-failover main-cpu** **Example:** `Router# configure terminal`	Forces a switchover on the active RP. The standby RP becomes the active RP with a switchover time of approximately 30 seconds or less. **Note** The modems do not redefine their ranges and the line cards do not reset during switchover.
Step 3	**show cable modem** **Example:** `Router> enable`	Displays information for the registered and unregistered cable modems supported by the newly active RP (formerly the standby RP).

Troubleshooting Route Processor Redundancy Plus

If RPR+ is not enabled after mode rpr-plus is run, verify that both the active and standby RPs are running Cisco IOS Release 12.2(11)BC3 or a later release.

Note If the active RP detects a different version of the image on the standby RP, the system automatically reverts to standard RPR behavior.

Configuration Examples for Route Processor Plus Redundancy

This section provides the following command examples that display the configuration and status of RPR+ on a Cisco uBR10012 router chassis with active and standby RPs. These commands all illustrate the same Cisco uBR10012 chassis:

- show redundancy
- show running configuration
- show version

The following show redundancy command displays the slots for the primary RP (PRE in slot 15), the secondary RP (PRE in slot 7), and additional redundancy mode information.

```
Router# show redundancy
Primary PRE in slot 15:
Secondary PRE in slot 7:
Preferred PRE: 15
Operating Redundancy Mode: RPR Plus
```

```
Auto synch: startup-config running-config
switchover timer 8 seconds [default]
```

The following show running configuration command displays RPR+ information such as main-cpu and auto-sync status.

```
Router# show run
Building configuration...
Current configuration : 10895 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
!
hostname "Router"
!
boot system flash bootflash:ubr10k-k8p6-mz.999-99.122BC_UB_030303
redundancy
 no keepalive-enable
 main-cpu
  auto-sync standard
no logging rate-limit
enable password cisco
!
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm intake-temperature critical 57
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
facility-alarm core-temperature critical 60
card 1/0 1gigethernet-1
card 1/1 2cable-tccplus
card 3/0 1oc12pos-1
card 4/0 1gigethernet-1
card 5/0 2cable-mc28c
card 5/1 cable-lcp
card 6/0 2cable-mc28c
card 7/0 2cable-mc28c
card 8/0 1cable-mc16s
card 8/1 1cable-mc16s
cable modem max-cpe unlimited
cable spectrum-group 1 band 8000000 20000000
cable modulation-profile 1 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 1 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 1 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable service flow inactivity-threshold
cable time-server
ip subnet-zero
ip cef table resolution-timer 1
no ip domain lookup
ip host abrick 223.255.254.254
ip dhcp relay information option
!
ip dhcp pool modems-c6
   network 1.6.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.10.41.3
```

```
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.6.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c5
   network 1.5.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.5.1.65
   default-router 1.5.1.65
   option 7 ip 1.5.1.65
   option 4 ip 1.5.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c7
   network 1.7.1.64 255.255.255.224
   bootfile up2-down2-nobpi.cm
   next-server 1.10.41.3
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.7.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c8
   network 1.8.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.8.1.65
   default-router 1.8.1.65
   option 7 ip 1.8.1.65
   option 4 ip 1.8.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c51
   network 1.9.1.64 255.255.255.224
   bootfile config.cm
   next-server 1.10.41.3
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.9.1.65
   option 2 hex ffff.8f80
!
ip multicast-routing
!
!
interface Loopback1
 ip address 222.1.1.1 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 1.10.41.3 255.255.0.0
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no cdp enable
!
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.0.0
 no negotiation auto
 no cdp enable
!
interface POS3/0/0
 ip address 200.200.0.1 255.255.0.0
 shutdown
 crc 32
 no cdp enable
 pos ais-shut
!
interface GigabitEthernet4/0/0
 no ip address
 negotiation auto
 no cdp enable
!
interface Cable5/0/0
```

```
 no ip address
 load-interval 30
 no keepalive
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 no cable upstream 0 concatenation
 cable upstream 0 data-backoff automatic
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 working 5
 hccp 1 channel-switch 5 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 1 channel-switch 5 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 1 reverttime 6
!
interface Cable5/0/0.1
 ip address 111.111.111.1 255.255.255.0 secondary
 ip address 1.5.1.65 255.255.255.224
 ip pim sparse-mode
 ip helper-address 1.10.41.3
 ip igmp static-group 239.0.0.11
 ip igmp static-group 239.0.0.12
 ip igmp static-group 239.0.0.14
 ip igmp static-group 239.0.0.16
 ip igmp static-group 239.0.0.32
 ip igmp static-group 239.0.0.35
 ip igmp static-group 239.0.0.36
 cable source-verify dhcp
 cable dhcp-giaddr policy
!
interface Cable5/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable6/0/0
 no ip address
 no keepalive
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 70
 cable upstream 0 frequency 12000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 working 6
 hccp 1 channel-switch 6 uc wavecom-ma 1.10.41.6 2 1.10.41.5 2
 hccp 1 channel-switch 6 nru rfswitch-group 1.10.41.7 80080000 2
!
```

```
interface Cable6/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable7/0/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 power-level 0
 no cable upstream 0 concatenation
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 protect 5 222.1.1.1
 hccp 1 channel-switch 5 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 1 channel-switch 5 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 1 protect 6 222.1.1.1
 hccp 1 channel-switch 6 uc wavecom-ma 1.10.41.6 2 1.10.41.5 2
 hccp 1 channel-switch 6 nru rfswitch-group 1.10.41.7 80080000 2
 hccp 1 timers 5000 15000
!
interface Cable7/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable8/0/0
 no ip address
 ip access-group 99 in
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 cable upstream 0 modulation-profile 2 1
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 threshold  cnr-profile1 21 cnr-profile2 11 Corr-Fec 11 Uncorr-Fec 21
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
 hccp 2 working 8
 hccp 2 channel-switch 8 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 2 channel-switch 8 nru rfswitch-group 1.10.41.7 80080000 1
!
```

```
interface Cable8/0/0.1
 ip address 1.8.1.65 255.255.255.224
 cable source-verify dhcp
!
interface Cable8/1/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable upstream 4 power-level 0
 cable upstream 4 shutdown
 cable upstream 5 power-level 0
 cable upstream 5 shutdown
 hccp 2 protect 8 222.1.1.1
 hccp 2 channel-switch 8 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 2 channel-switch 8 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 2 timers 5000 15000
 no hccp 2 revertive
!
ip default-gateway 1.10.0.1
ip classless
ip route 1.9.0.0 255.255.0.0 1.10.0.1
ip route 2.6.0.0 255.255.0.0 200.200.0.2
ip route 223.255.254.254 255.255.255.255 1.10.0.1
no ip http server
ip pim bidir-enable
!
ip access-list standard XYZ
 permit any
ip access-list standard pqRS
 permit any
no logging linecard
access-list 3 permit 210.221.55.46
access-list 99 permit any
access-list 110 permit ip any any
access-list 110 permit udp any eq bootps any
access-list 111 permit udp any eq bootps any
arp 1.10.41.6 0020.4a51.1776 ARPA
arp 1.10.41.5 0020.4a51.00ea ARPA
no cdp run
snmp-server manager
tftp-server bootflash:up2-down2-nobpi.cm alias up2-down2-nobpi.cm
tftp-server bootflash:tony11.cm alias tony11.cm
tftp-server bootflash:up2-down2.cm alias up2-down2.cm
tftp-server bootflash:new-privacy.cm alias new-privacy.cm
tftp-server bootflash:10.cm alias 10.cm
tftp-server bootflash:att-10plus.cm alias att-10plus.cm
tftp-server bootflash:schcfr_new.cm alias schcfr_new.cm
tftp-server bootflash:test11.cm alias test11.cm
tftp-server bootflash:4us16ds.cm alias 4us16ds.cm
!
alias exec scm show cable modem
alias exec sqos show cable qos profile
alias exec shc show hccp
alias exec nd no debug all
alias exec sr show running-config
alias exec sip show ip interface b
alias exec dc debug hccp channel-switch
alias exec spm sh proc mem | in HCCP
alias exec de debug hccp event
alias exec ds debug hccp sync
alias exec dp debug hccp plane
```

```
alias exec dt debug hccp timing
alias exec dipc debug cr10k-rp ipc
alias exec dpm debug hccp plane message
alias exec dpp debug hccp plane packet
alias exec sib show ip int br
alias exec shb show hccp br
alias exec scs show cable spectrum-group
!
line con 0
 exec-timeout 0 0
line aux 0
 stopbits 1
 speed 19200
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 length 0
!
end
```

The following show version command displays active and standby RP status.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K-K8P6-M), Version 12.2(122BC.030303.)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 03-Mar-03 21:23 by
Image text-base: 0x60008954, data-base: 0x61B00000
ROM: System Bootstrap, Version 12.0(9r)SL2, RELEASE SOFTWARE (fc1)
amit-rp2 uptime is 57 minutes
System returned to ROM by reload at 02:05:40 UTC Sun Nov 26 2000
System image file is "bootflash:ubr10k-k8p6-mz.999-99.122BC_UB_030303"
cisco uBR10000 (PRE1-RP) processor with 393215K/131072K bytes of memory.
Processor board ID TBA05191959
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
Backplane version 1.0, 8 slot
Last reset from other pre
Toaster processor tmc0 is running.
Toaster processor tmc1 is running.
1 OC12 POS controller (1 POS)
1 TCCplus card(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Gigabit Ethernet/IEEE 802.3 interface(s)
1 Packet over SONET network interface(s)
8 Cable Modem network interface(s)
509K bytes of non-volatile configuration memory.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
32768K bytes of Flash internal SIMM (Sector size 256KB).
Secondary is up.
Secondary has 524288K bytes of memory.
Configuration register is 0x0
```

Additional References

Related Documents

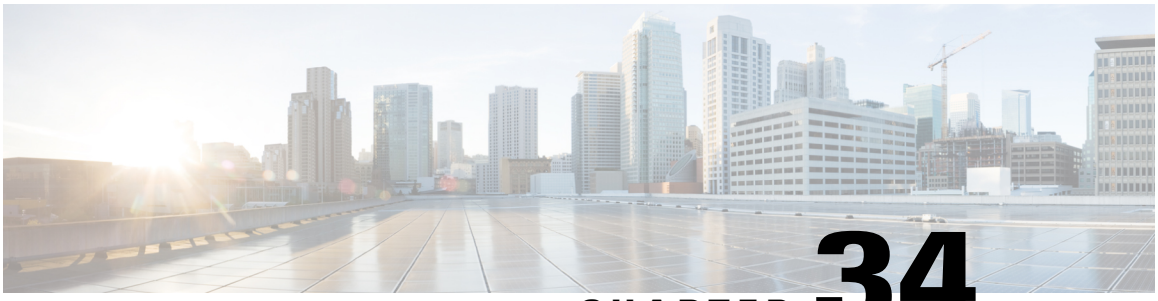
Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
CMTS Software Configuration Guide Guide	Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC
Cisco High Availability Initiatives	

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

PART V

Layer 2 and VPN Features



CHAPTER 34

EtherChannel for the Cisco Cable Modem Termination System

First Published: February 14, 2008

This document describes the features, benefits and configuration of Cisco EtherChannel technology on the Cisco Cable Modem Termination System (CMTS).

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

EtherChannel is a technology by which to configure and aggregate multiple physical Ethernet connections to form a single logical port with higher bandwidth. The first EtherChannel port configured on the Cisco CMTS serves as the EtherChannel bundle master by default, and each slave interface interacts with the network using the MAC address of the EtherChannel bundle master.

EtherChannel ports reside on a routing or bridging end-point. The router or switch uses EtherChannel to increase bandwidth utilization in either half- or full-duplex mode, and load balances the traffic across the multiple physical connections.

EtherChannel on the Cisco CMTS supports inter-VLAN routing with multiple devices and standards, and supports FastEtherChannel (FEC) and Gigabit EtherChannel (GEC) on the Cisco CMTS depending on the router and associated processing modules in the chassis.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for EtherChannel on the Cisco CMTS

The Cisco uBR10012 universal broadband router has the following prerequisites to support GEC and 802.1Q encapsulation for inter-VLAN trunking, also summarized in the table:

- Cisco IOS Release 12.2(9a)BC or a later BC release.
- The Cisco uBR10012 router supports only GEC with PRE2 and PRE4 performance routing engine modules.

The Cisco uBR7246VXR universal broadband router has the following prerequisites to support FEC or GEC and 802.1Q encapsulation for inter-VLAN trunking:

- Cisco IOS Release 12.2(11)BC3 or a later BC release.
- The Cisco uBR7246VXR router supports FEC on Fast Ethernet channels with the Cisco NPE-225 or Cisco NPE-400 network processing engines.
- The Cisco uBR7246VXR router supports GEC on Gigabit Ethernet channels using the Cisco uBR7200-NPE-G1 network processing engine.

Table 97: Supported Interfaces and Encapsulations for EtherChannel on the Cisco CMTS

Cisco CMTS	Full Duplex Supported	Encapsulation Supported	Cisco IOS Release
Cisco uBR7246VXR	Fast Ethernet with the Cisco NPE-225 or Cisco NPE-400	IEEE 802.1Q	12.2(11)BC3
	GigabitEthernet with the Cisco uBR7200-NPE-G1	IEEE 802.1Q	12.2(9a)BC
Cisco uBR10012	Gigabit Ethernet with the PRE2 Module	IEEE 802.1Q	12.2(9a)BC
Cisco uBR10012	Gigabit Ethernet with the PRE4 Module	IEEE 802.1Q	12.2(33)BC

Restrictions for EtherChannel on the Cisco CMTS

The following restrictions apply to both the Cisco uBR10012 and Cisco uBR7246VXR routers with Cisco IOS Release 12.2(9a)BC and earlier supported releases, and Cisco IOS Release 12.2(33)SCA and later releases:

- EtherChannel on the Cisco CMTS is limited to Network Layer 3 functions, and does not support Data-Link Layer 2 EtherChannel functions as with certain other Cisco product platforms.
- The Port Aggregation Protocol (PAgP) is not supported on the Cisco CMTS as with other Cisco product platforms (such as the CatOS switch).
- Only the IEEE 802.1Q trunking protocol is supported on the Cisco CMTS. ATM trunking is not supported on the Cisco uBR10012 or Cisco uBR7246VXR routers as of this release.
- The maximum supported links per bundle is 8.
- EtherChannel on Cisco CMTS supports only physical ports or interfaces that have the same speed.
- Starting Cisco IOS Release 12.2(33)BC, EtherChannel on the Cisco uBR10012 router does not support MQC QOS. You can use Equal Cost Multi Path (ECMP) load balancing instead of EtherChannel.
- Layer 3 configurations on member interfaces of EtherChannel are not supported.
- Port Channel configuration is not supported on Gigabit Ethernet interface of Cisco uBR-MC3GX60 line card.
- MAC Address Accounting feature on port channel is not supported.

Information About EtherChannel on the Cisco CMTS

Several Cisco product platforms currently support EtherChannel, such as the Cisco 7200 Series and Cisco Catalyst Switches. This document describes EtherChannel on the following Cisco CMTS router platforms:

Introduction to EtherChannel on the Cisco CMTS

EtherChannel is based on proven industry-standard technology. The Cisco CMTS supports EtherChannel with several benefits, including the following:

- EtherChannel on the Cisco CMTS supports subsecond convergence times.
- EtherChannel can be used to connect two switch devices together, or to connect a router with a switch.
- A single EtherChannel connection supports a higher bandwidth between the two devices.
- The logical port channels on either Cisco CMTS platform provide fault-tolerant, high-speed links between routers, switches, and servers.
- EtherChannel offers redundancy and high availability on the Cisco CMTS. Failure of one connection causes a switch or router to use load balancing across the other connections in the EtherChannel.
- Load balancing on the Cisco CMTS supports dynamic link addition and removal without traffic interruption.
- EtherChannel supports inter-VLAN trunking. Trunking carries traffic from several VLANs over a point-to-point link between the two devices. The network provides inter-VLAN communication with

trunking between the Cisco CMTS router and one or more switches. In a campus network, trunking is configured over an EtherChannel link to carry the multiple VLAN information over a high-bandwidth channel.

Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router

Cisco's Fast EtherChannel (FEC) technology builds upon standards-based 802.3 full-duplex Fast Ethernet to provide a reliable high-speed solution for network managers who require higher bandwidth between servers, routers, and switches than single-link Ethernet technology can provide.

Fast EtherChannel provides bandwidth scalability within the network backbone by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity available on an increasing number of platforms.

Fast EtherChannel technology solves the immediate problem of scaling bandwidth within the network backbone, and can be applied to support Gigabit EtherChannels.

Cisco IOS Release 12.2(11)BC3 introduced support for Cisco EtherChannel technology for the Cisco uBR7246VXR router, and support continues with Cisco IOS Release 12.2(9a)BC. FEC on the Cisco uBR7246VXR router includes the following EtherChannel capabilities:

- Supports a maximum of four physical ports to be combined into one logical FEC or GEC link.
- Supports bandwidth up to 800 Mbps FEC (Fast EtherChannel full duplex) on the Cisco uBR7246VXR router.
- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half-duplex) for a combined total of up to 8 Gbps (full-duplex) with the Cisco uBR7200-NPE-G1 processor.

The Cisco uBR7200-NPE-G1 processor includes three onboard Gigabit Ethernet interfaces. If you want to use these interfaces to replace the Fast Ethernet interfaces on the existing I/O controller, you will have to configure the new interfaces before they can be used to access the network. If you are also removing the existing I/O controller, you remove the configuration for its Fast Ethernet interfaces.

The Cisco uBR7200-NPE-G1 contains its own onboard I/O controller, which includes the boot flash memory and NVRAM memory. After you install the Cisco uBR7200-NPE-G1 in a chassis, you can no longer access the boot flash and NVRAM memory on the I/O controller. You must therefore copy the Cisco IOS software image and configuration file to the memory on the Cisco uBR7200-NPE-G1.

Cisco GigabitEtherChannel (GEC) on the Cisco uBR10012 Router

Cisco GigabitEtherChannel (GEC) is high-performance Ethernet technology that provides gigabit-per-second transmission rates. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers.

Cisco IOS Release 12.2(9a)BC supports GigabitEtherChannel on the Cisco uBR10012 router with the following EtherChannel capabilities:

- Supports IEEE 802.1Q encapsulation for inter-VLAN networking.
- Supports a maximum of four physical Ethernet ports to be combined as one logical EtherChannel link.
- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half duplex) for a combined total of up to 8 Gbps (full duplex) on the Cisco uBR10012 router with PRE2 performance routing engine modules.

How to Configure EtherChannel on the Cisco CMTS

This section contains the following:

Configuring FEC or GEC EtherChannel on the Cisco CMTS

This procedure describes and illustrates the configuration of EtherChannel FEC or GEC on the Cisco uBR7246VXR or Cisco uBR10012 routers, subject to the prerequisites

Before You Begin

- Cisco IOS 12.2(9a)BC is installed or upgraded on either the Cisco uBR10012 or Cisco uBR7246VXR universal broadband router.
- Fast Ethernet or Gigabit Ethernet modules and interfaces are installed on the Cisco uBR7246VXR chassis as described in the "Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router" section on page 4 .
- PRE2 modules are installed in the Cisco uBR10012 router chassis as described in Cisco GEC on Cisco CMTS.
- Fast Ethernet or Gigabit Ethernet cabling is completed and the ports are operational on the router and network.
- LAN interfaces are configured and operational on the router and network, with IP addresses and subnet masks.

Note

- The Cisco uBR7246VXR and Cisco uBR10012 routers support up to four physical connectors to be configured as one logical FEC or GEC port.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface port-channel** *n* **Example:** `Router(config)# interface port-channel 1`	Creates an EtherChannel interface. The first EtherChannel interface configured becomes the bundle master for all ports in the EtherChannel group. The MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. • n—EtherChannel port number for the specified port. The EtherChannel port number may range from 1 to 64. To remove an EtherChannel interface from the EtherChannel group, use the no form of this command. For illustration, the example at left names the interface **Port-channel1**. If the first EtherChannel interface in the group is later removed, the second EtherChannel interface in the group becomes the bundle master by default. Repeat this step on every EtherChannel port to be bundled into a FEC or GEC group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode for **Port-channel1** and returns to global configuration mode.
Step 5	**interface gigabitethernet** *slot/{subslot}/port* **Example:** `Router# interface gigabitethernet 1/0/0`	(Gigabit Ethernet interface only) Selects the Gigabit Ethernet interface that you wish to add as a member EtherChannel link in the EtherChannel bundle, and enters interface configuration mode. The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: • ◦ slot/subslot/port—Cisco uBR10012 router ◦ slot/port—Cisco uBR7246VXR router **Note** Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel. Use the shutdown command in interface configuration mode immediately before completing the following steps in this procedure.
Step 6	**interface fastethernet** *slot/(subslot}port* **Example:** `Router# interface fastethernet 3/0`	(Fast Ethernet interface only) Selects a Fast Ethernet interface and enters interface configuration mode. **Note** The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: • ◦ slot/subslot/port—Cisco uBR10012 router ◦ slot/port—Cisco uBR7246VXR router

	Command or Action	Purpose
Step 7	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 5 or Step 6 above prior to configuring it as a member of the EtherChannel. **Note** Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel.
Step 8	**channel-group** *number* **Example:** `Router(config-if)# channel-group 1`	Adds the current interface (Gigabit Ethernet or Fast Ethernet) to the EtherChannel Group, associating that interface with an EtherChannel link. • number—The identifying number for the EtherChannel group with which to associate this interface. An EtherChannel group can be identified in the range of 1 to 64, and each group can have up to four interfaces, only one of which is the master. To remove an EtherChannel group and the associated ports from the Cisco CMTS, use the no form of this command.
Step 9	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which EtherChannel is configured.
Step 10	**Ctrl-Z** **Example:** `Router(config# Ctrl-z`	Returns to privileged EXEC mode. IP traffic should be visible on the network with completion of the above steps.

Troubleshooting Tips

Once interface operations are confirmed (prior to this procedure), and EtherChannel configurations have been verified (next procedure), any difficulty experienced through the EtherChannel links may pertain to inter-VLAN or IP routing on the network, or perhaps very high bandwidth consumption.

See the "Additional References" section on page 10 for further resources in troubleshooting these and additional configurations.

What to Do Next

Additional IP, access list, inter-VLAN or load balancing configurations may be made to the Cisco CMTS and these changes will be supported in the running EtherChannel configuration without service disruption from EtherChannel.

Refer to the "Additional References" section on page 11 for more information.

Verifying EtherChannel on the Cisco CMTS

Links can be added or removed from an EtherChannel interface without traffic interruption. If an Ethernet link in an EtherChannel interface fails, traffic previously carried over the failed link switches to the remaining links within the EtherChannel. There are a number of events that can cause a link to be added or removed including adding or removing a link using commands and simulating link failure and recovery (as with (no)shutdown links).

Cisco EtherChannel supports online insertion and removal (OIR) of field-replaceable units (FRUs) in the Cisco CMTS chassis. Ports that remain active during OIR of one FRU will take over and support the traffic bandwidth requirements without service disruption. However, OIR is not described in this procedure.

Refer to the "Additional References" section on page 10 for complete OIR procedures and guidelines for the respective FRU.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface port-channel** *n* **Example:** `Router# show interface port-channel 1`	Verifies the EtherChannel configuration on the Cisco CMTS for the selected EtherChannel group. • n—The identifying number for the Port Channel group to display.

Configuration Examples for EtherChannel on the Cisco CMTS

The sequential configuration example and commands in Table 2 illustrate the configuration of Etherchannel on a Cisco uBR7246VXR router with a five-port sensor:

The following example illustrates Gigabit EtherChannel (GEC) information for the port-channel interface of 2 as configured on a Cisco uBR10012 router with the PRE2 performance routing engine model.

This configuration is comprised of three GEC port channels as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```
Router# show interface port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 8888.8888.8888 (bia 0000.0000.0000)
  Internet address is 101.101.101.1/16
```

```
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured  members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
        Member 0 : GigabitEthernet1/0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s
        Member 2 : GigabitEthernet2/0/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17292000 bits/sec, 9948 packets/sec
  30 second output rate 17315000 bits/sec, 9935 packets/sec
     866398790 packets input, 3324942446 bytes, 0 no buffer
     Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     866394055 packets output, 3323914794 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The following example illustrates GEC information for the port-channel interface of 2 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of three port-channel interfaces (members) as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```
Router# show interfaces port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 000b.bf7d.9c01 (bia 000b.bf7d.9c00)
  Internet address is 101.101.101.2/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured  members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
        Member 0 : GigabitEthernet0/3 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet0/2 , Full-duplex, 1000Mb/s
        Member 2 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:13:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17358000 bits/sec, 9999 packets/sec
  30 second output rate 17359000 bits/sec, 10000 packets/sec
     868633935 packets input, 3809968911 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 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     868642883 packets output, 3811242413 bytes, 0 underruns
     2 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The following example illustrates FastEtherChannel (FEC) information for the port channel interface of 1 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of four port channel interfaces (members) as follows:

- Member 0
- Member 0 is the GEC interface bundle master.
- Member 3 is the final slave interface in this FEC group.
- These four port-channel interfaces (members) comprise one FEC group that is set up with an FEC peer on the network.

```
Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 000b.bf7d.9c1c (bia 000b.bf7d.9c00)
  Description: test
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec,
     reliability 255/255, txload 11/255, rxload 11/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 4
    No. of configured  members in this channel: 4
    No. of passive members in this channel: 0
    No. of active members in this channel: 4
        Member 0 : FastEthernet2/1 , Full-duplex, 100Mb/s
        Member 1 : FastEthernet2/0 , Full-duplex, 100Mb/s
        Member 2 : FastEthernet1/1 , Full-duplex, 100Mb/s
        Member 3 : FastEthernet1/0 , Full-duplex, 100Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:14:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/160 (size/max)
  30 second input rate 17358000 bits/sec, 9998 packets/sec
  30 second output rate 17357000 bits/sec, 9998 packets/sec
     869366601 packets input, 3968956491 bytes
     Received 3 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
     868944538 packets output, 3876736548 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Additional References

Related Documents

Related Topic	Document Title
EtherChannel for Cisco Products	• Cisco EtherChannel home page http://www.cisco.com/warp/public/cc/techno/lnty/etty/fsetch/index.shtml • Cisco EtherChannel Technology white paper http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml
Cisco uBR10012 Universal Broadband Router	• Cisco uBR10012 Universal Broadband Router Hardware Installation Guide http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/installation/guide/hig.html • Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module http://www.cisco.com/c/en/us/td/docs/interfaces_modules/cable/performance_routing_engine/installation/guide/pre5096.html • Cisco uBR10012 OC-48 DPT/POS Interface Module (Installation and Configuration) http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/installation/field_replaceable_units/ub_oc48.html

Related Topic	Document Title
Cisco uBR7246VXR Universal Broadband Router	• Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html • Cisco uBR7246VXR Universal Broadband Router Performance Routing Engine Module http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/ubr7246vxr/upgrade/guide/15066R.html http://www.cisco.com/en/US/products/hw/modules/ps4917/products_white_paper09186a0080113728.shtml
WAN and Inter-VLAN Routing with the Cisco CMTS	• Configuring LAN Interfaces chapter in the Cisco IOS Interface Configuration Guide , Release 12.2 http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflanin.html • Point-to-Point Protocol over Ethernet Support on the Cisco CMTS http://www.cisco.com/c/en/us/td/docs/cable/cmts/feature/guide/cmtsfg/ufgpppoe.html • ATM Multilink PPP Support on Multiple Virtual Circuits (VCs) http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/atm/configuration/12-2sx/atm-12-2sx-book/atm-ml-ppp-mul-vc.html • Cisco New Virtual Circuit (VC) Configuration Virtual Circuits

Related Topic	Document Title
Configuring Additional Devices for EtherChannel	• *Configuring EtherChannel and 802.1Q Trunking Between a Catalyst 2950 and a Router (inter-VLAN Routing)* http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html • *Configuring EtherChannel and 802.1Q Trunking Between Catalyst 2900XL/3500XL and Catalyst 2940, 2950/2955, and 2970 Switches* http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/21041-131.html

Standards and RFCs

Standards	Title
IEEE Std 802.1Q, 2003 Edition	IEEE Std 802.1Q, 2003 Edition (Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u-2001, IEEE Std 802.1v-2001, and IEEE Std 802.1s-2002) http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=27089

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support

Feature Information for EtherChannel on the Cisco CMTS

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 98: Feature Information for EtherChannel on the Cisco CMTS

Feature Name	Releases	Feature Information
GEC Support on the Cisco uBR10012 universal broadband router	12.2(9a)BC	GEC support was introduced on the Cisco uBR10012 universal broadband router with the Cisco uBR10012 PRE2 performance routing engine.
FEC and GEC Support on the Cisco uBR7246VXR router	12.2(11)BC3	FEC and GEC support was introduced on the Cisco uBR7246VXR router with the NPE-G1 network processing engine required for GEC. The following commands are introduced or modified in the feature or features documented in this module. • **channel-group** • **interface port-channel** • **show interface port-channel**

CHAPTER 35

Cisco uBR7200 Series MPLS VPN Cable Enhancements

First Published: February 14, 2008

This feature module describes the Cisco uBR7200 series universal broadband router cable Multiprotocol Label Switching Virtual Private Network (MPLS VPN) and cable interface bundling features. It explains how to create a VPN using MPLS protocol, cable subinterfaces, and interface bundles. VPNs can be created in many ways using different protocols.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Feature Overview

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.

The cable MPLS VPN network consists of:

- 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 only to 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 BGP and IP address resolution to ensure security. See *Configuring Multiprotocol Label Switching*.

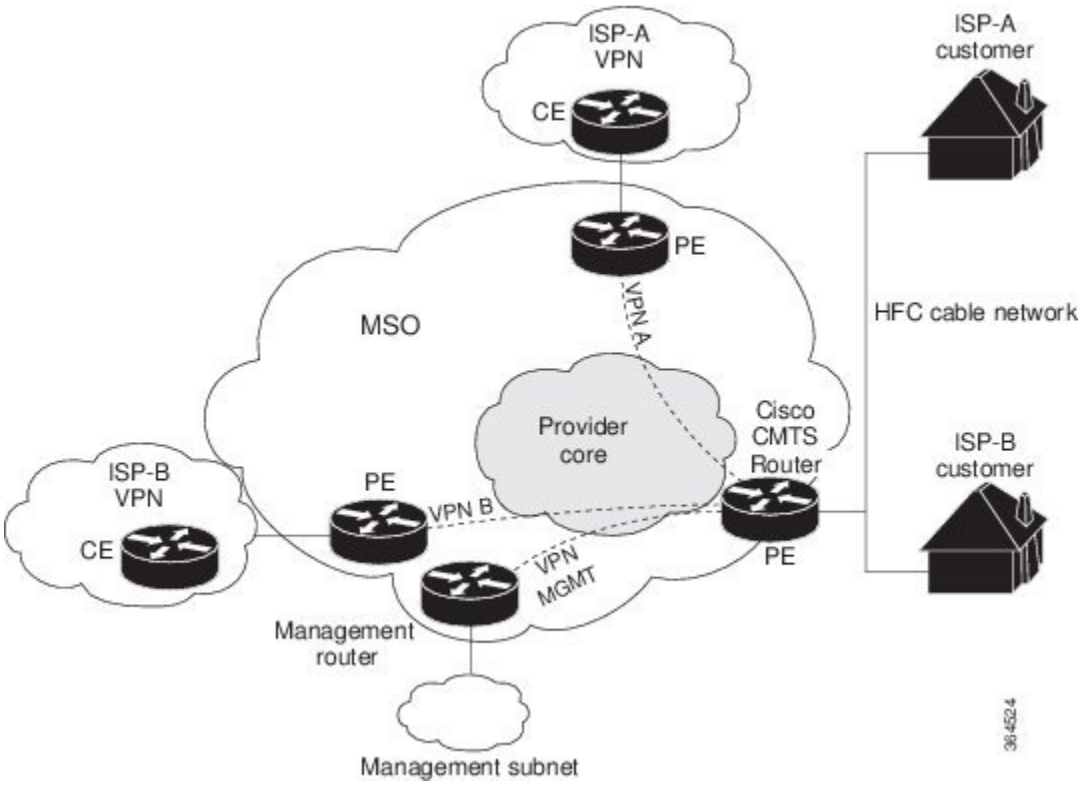
The table shows a cable MPLS VPN network. The routers in the network are:

- Provider (P) router—Routers in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- Provider Edge (PE) router— Router that adds the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router. In the MPLS-VPN approach, each Cisco CMTS router acts as a PE router.
- Customer (C) router—Router in the ISP or enterprise network.
- Customer Edge (CE) router—Edge router on the ISP's network that connects to the PE router on the MSO's network. A CE router must interface with a PE router.

The MPLS network has a unique VPN that exclusively manages the MSOs devices called the management VPN. It contains servers and devices that other VPNs can access. The management VPN connects the Cisco CMTS router to a PE router, which connects to management servers such as Cisco Network Registrar (CNR) and Time of Day (ToD) servers. A PE router connects to management servers and is a part of the management VPN. Regardless of the ISP they belong to, the management servers serve the Dynamic Host Configuration Protocol (DHCP), DNS (Domain Name System), and TOD requests coming from PCs or cable modems.

Note When configuring MPLS VPNs, you must configure the first subinterface created as a part of the management VPN.

Figure 22: MPLS VPN Network



Cable VPN configuration involves an:

- MSO domain that requires a direct peering link to each enterprise network (ISP), provisioning servers for residential and commercial subscribers, and dynamic DNS for commercial users. The MSO manages cable interface IP addressing, Data-over-Cable Service Interface Specifications (DOCSIS) provisioning, CM hostnames, routing modifications, privilege levels, and usernames and passwords.
- ISP or enterprise domain that includes the DHCP server for subscriber or telecommuter host devices, enterprise gateway within the MSO address space, and static routes back to the telecommuter subnets.

Note Cisco recommends that the MSO assign all addresses to the end user devices and gateway interfaces. The MSO can also use split management to let the ISP configure tunnels and security.

In an MPLS VPN configuration, the MSO must configure the following:

- CMTS
- P routers

- PE routers
- CE routers
- One VPN per ISP DOCSIS servers for all cable modem customers. The MSO must attach DOCSIS servers to the management VPN, and make them visible.

The MSO must configure the Cisco CMTS routers that serve the ISP, and remote PE routers connecting to the ISP, as PE routers in the VPN.

The MSO must determine the primary IP address range for all cable modems.

The ISP must determine the secondary IP address range for subscriber PCs.

To reduce security breaches and differentiate DHCP requests from cable modems in VPNs or under specific ISP management, MSOs can use the **cable helper-address** command in Cisco IOS software. The MSO can specify the host IP address to be accessible only in the ISP's VPN. This lets the ISP use its DHCP server to allocate IP addresses. Cable modem IP address must be accessible from the management VPN.

The MPLS VPN approach of creating VPNs for individual ISPs or customers requires subinterfaces to be configured on the virtual bundle interface. Each ISP requires one subinterface. The subinterfaces are tied to the VPN Routing/Forwarding (VRF) tables for their respective ISPs. The first subinterface must be created on the cable interface bound to the management VPN.

To route a reply from the CNR back to the cable modem, the PE router that connects to the CNR must import the routes of the ISP VPN into the management VPN. Similarly, to forward management requests (such as DHCP renewal to CNR) to the cable modems, the ISP VPN must export and import the appropriate management VPN routes.

You can group all of the cable interfaces on a Cisco CMTS router into a single bundle so that only one subnet is required for each router. When you group cable interfaces, no separate IP subnet or each individual cable interface is required. This grouping avoids the performance, memory, and security problems in using a bridging solution to manage subnets, especially for a large number of subscribers.

Subinterfaces allow traffic to be differentiated on a single physical interface, and assigned to multiple VPNs. You can configure multiple subinterfaces, and associate an MPLS VPN with each subinterface. You can split a single physical interface (the cable plant) into multiple subinterfaces, where each subinterface is associated with a specific VPN. Each ISP requires access on a physical interface and is given its own subinterface. Create a management subinterface to support cable modem initialization from an ISP.

Using each subinterface associated with a specific VPN (and therefore, ISP) subscribers connect to a logical subinterface, which reflects the ISP that provides their subscribed services. When properly configured, subscriber traffic enters the appropriate subinterface and VPN.

Benefits

- MPLS VPNs give cable MSOs and ISPs a manageable way of supporting multiple access to a cable plant. Service providers can create scalable and efficient VPNs across the core of their networks. MPLS VPNs provide systems support scalability in cable transport infrastructure and management.
- Each ISP can support Internet access services from a subscriber's PC through an MSO's physical cable plant to their networks.
- MPLS VPNs allow MSOs to deliver value-added services through an ISP, and thus, deliver connectivity to a wider set of potential customers. MSOs can partner with ISPs to deliver multiple services from multiple ISPs and add value within the MSO's own network using VPN technology.

- Subscribers can select combinations of services from various service providers.
- The MPLS VPN cable features set build on CMTS DOCSIS 1.0 and DOCSIS 1.0 extensions to ensure services are reliably and optimally delivered over the cable plant. MPLS VPN provides systems support domain selection, authentication per subscriber, selection of QoS, policy-based routing, and ability to reach behind the cable modem to subscriber end devices for QoS and billing while preventing session spoofing.
- MPLS VPN technology ensures both secure access across the shared cable infrastructure and service integrity.
- Cable interface bundling eliminates the need for an IP subnet on each cable interface. Instead, an IP subnet is only required for each cable interface bundle. All cable interfaces in a Cisco CMTS router can be added to a single bundle.

Restrictions

- Each subinterface on the CMTS requires an address range from the ISP and from the MSO. These two ranges must not overlap and must be extensible to support an increased number of subscribers for scalability.

Note This document does not address allocation and management of MSO and ISP IP addresses. See *Configuring Multiprotocol Label Switching* for this information.

- The **cable source-verify dhcp** command enables Dynamic Host Control Protocol (DHCP) Lease query protocol from the CMTS to DHCP server to verify IP addresses of upstream traffic, and prevent MSO customers from using unauthorized, spoofed, or stolen IP addresses.
- When using only MPLS VPNs, create subinterfaces on the virtual bundle, assign it an IP address, and provide VRF configuration for each ISP. When you create subinterfaces and configure only MPLS VPNs, the cable interface bundling feature is independent of the MPLS VPN.
- When using cable interface bundling:
  - Define a virtual bundle interface and associate any cable physical interface to the virtual bundle.
  - Specify all generic IP networking information (such as IP address, routing protocols, and switching modes) on the virtual bundle interface. Do not specify generic IP networking information on bundle slave interfaces.
  - An interface that has a subinterface(s) defined over it is not allowed to be a part of the bundle.
  - Specify generic (not downstream or upstream related) cable interface configurations, such as source-verify or ARP handling, on the virtual bundle interface. Do not specify generic configuration on bundle slave interfaces.
- Interface bundles can only be configured using the command line interface (including the CLI-based HTML configuration).

Supported Platforms

- Cisco uBR7223
- Cisco uBR7246
- Cisco uBR7246 VXR

Prerequisites

Before configuring IP-based VPNs, complete the following tasks:

- Ensure your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified based on National Television Standards Committee (NTSC) or appropriate international cable plant recommendations. Ensure your plant meets all DOCSIS or European Data-over-Cable Service Interface Specifications (EuroDOCSIS) downstream and upstream RF requirements.
- Ensure your Cisco router is installed following instructions in the Hardware Installation Guide and the Regulatory Compliance and Safety Information guide.
- Ensure your Cisco router is configured for basic operations.
- The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable modem card to serve as the RF cable TV interface.

Other Important Information

- Ensure all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational based on the services to support. This includes all routers, servers (DHCP, TFTP, and ToD), network management systems, other configuration or billing systems and backbone, and other equipment to support VPN.
- Ensure DHCP and DOCSIS configuration files have been created and pushed to appropriate servers such that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TFTP and ToD server addresses, and download a DOCSIS configuration file. Configure each subinterface to connect to the ISP's VPN.
- Ensure DOCSIS servers are visible on the management VPN.
- Be familiar with your channel plan to assign appropriate frequencies. Outline your strategies for setting up bundling or VPN solution sets if applicable to your headend or distribution hub. Obtain passwords, IP addresses, subnet masks, and device names as appropriate.
- Create subinterfaces off of a virtual bundle interface. Configure each subinterface to connect to the ISP network.

The MPLS VPN configuration steps assume the following:

- IP addressing has already been determined and there are assigned ranges in the MSO and ISP network for specific subinterfaces.
- The MSO is using CNR and has configured it (using the **cable helper-address** command) to serve appropriate IP addresses to cable modems based on the cable modem MAC address. The CMTS forwards

DHCP requests to the CNR based on the **cable helper-address** settings. The CNR server determines the IP address to assign the cable modem using the client-classes feature, which let the CNR assign specific parameters to devices based on MAC addresses.

- ISP CE routers are configured (using the **cable helper-address** command) to appropriately route relevant IP address ranges into the VPN.
- P and PE routers are already running Cisco Express Forwarding (CEF).
- MPLS is configured on the outbound VPN using the **tag switching ip** command in interface configuration mode.

Configuration Tasks

To configure MPLS VPNs, perform the following tasks:

Creating VRFs for each VPN

To create VRFs for each VPN, perform the following steps beginning in the router configuration mode.

Note Since only the CMTS has logical subinterfaces, assignments of VRFs on the other PE devices will be to specific physical interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip vrf** *mgmt-vpn*	Enters VRF configuration mode (config-vrf)# and maps a VRF table to the VPN (specified by *mgmt-vpn*). The management VPN is the first VPN configured.
Step 2	Router(config-vrf)# **rd** *mgmt-rd*	Creates a routing and forwarding table by assigning a route distinguisher to the management VPN.
Step 3	Router(config-vrf)# **route-target** {**export**| **import**| **both**} *mgmt-rd*	Exports and/or imports all routes for the management VPNs route distinguisher. This determines which routes will be shared within VRFs.
Step 4	Router(config-vrf)# **route-target import** isp1-vpn-rd	Imports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 5	Router(config-vrf)# **route-target import** isp2-vpn-rd	Imports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 6	Router(config-vrf)# **ip vrf** isp1-vpn	Creates a routing and forwarding table by assigning a route distinguisher to *isp1-vpn* .
Step 7	Router(config-vrf)# **rd** *mgmt-rd*	Creates a routing and forwarding table by assigning a route distinguisher (mgmt-rd) to the management VPN (mgmt-vpn).

	Command or Action	Purpose
Step 8	Router(config-vrf)# **route-target export** isp1-vpn-rd	Exports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 9	Router(config-vrf)# **route-target import** isp1-vpn-rd	Imports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 10	Router(config-vrf)# **route-target import** mgmt-vpn-rd	Exports all routes for the VPNs (*mgmt-vpn)* route distinguisher.
Step 11	Router(config-vrf)# **ip vrf** isp2-vpn	Creates a routing and forwarding table by assigning a route distinguisher to *isp2-vpn* .
Step 12	Router(config-vrf)# **route-target export** isp2-vpn-rd	Exports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 13	Router(config-vrf)# **route-target import** isp2-vpn-rd	Imports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 14	Router(config-vrf)# **route-target import** mgmt-vpn-rd	Imports all routes for the VPNs (*mgmt-vpn)* route distinguisher.

Defining Subinterfaces on a Virtual Bundle Interface and Assigning VRFs

To create a logical cable subinterface, perform the following steps beginning in the global configuration mode. Create one subinterface for each VPN (one per ISP). The first subinterface created must be configured as part of the management VPN (with the lowest subinterface number).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters configuration mode.
Step 2	Router(config)# **interface bundle n**	Enters virtual bundle interface configuration mode and defines the first (management) subinterface with the lowest subinterface number. Valid range for the bundle number n is from 1 to 255.
Step 3	Router(config-subif)# **description** *string*	Identifies the subinterface as the management subinterface.
Step 4	Router(config-subif)# **ip vrf forwarding** *mgmt-vpn*	Assigns the subinterface to the management VPN (the MPLS VPN used by the MSO to supply service to customers).
Step 5	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.
Step 6	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 7	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.

	Command or Action	Purpose
Step 8	Router(config-if)# **interface bundle n**	Defines an additional subinterface for the ISP (such as isp1).
Step 9	Router(config-subif)# **description** *string*	Identifies the subinterface (such as subinterface for *isp1-vpn)* .
Step 10	Router(config-subif)# **ip vrf forwarding** *isp1-vpn*	Assigns the subinterface to *isp1-vpn* VPN.
Step 11	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.
Step 12	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 13	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.
Step 14	Router(config-if)# **interface cable** *slot/port.n*	Defines an additional subinterface for the ISP (such as isp2).
Step 15	Router(config-subif)# **description** *string*	Identifies the subinterface (such as subinterface for *isp2-vpn)* .
Step 16	Router(config-subif)# **ip vrf forwarding** *isp2-vpn*	Assigns the subinterface to *isp2-vpn* VPN.
Step 17	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.
Step 18	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 19	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.
Step 20	Router(config)# **exit**	Returns to configuration mode.

Configuring Cable Interface Bundles

To assign a cable interface to a bundle, perform the following steps beginning in the interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface cable** *slot/port*	Enters the cable interface configuration mode. IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 2	Router(config-if)# **cable bundle** *bundle-number* **[master]**	Defines the interface as the bundle's master interface.

	Command or Action	Purpose
Step 3	Router(config)# **interface cable** *slot/port*	Enters the cable interface configuration mode for another cable interface. IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 4	Router(config-if)# **cable bundle** *bundle-number*	Adds the interface to the bundle specified by *bundle-number* .

Configuring Subinterfaces and MPLS VPNs on a Virtual Bundle Interface

To configure subinterfaces on a virtual bundle interface and assign each subinterface a Layer 3 configuration:

Configure cable interface bundles.

Define subinterfaces on the virtual bundle interface and assign a Layer 3 configuration to each subinterface.

Create one subinterface for each customer VPN (one per ISP).

Configuring MPLS in the P Routers in the Provider Core

To configure MPLS in the P routers in the provider core, perform the following steps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters configuration mode.
Step 2	Router(config)#**ip cef**	Enables Cisco Express Forwarding (CEF) operation. For information about CEF configuration and command syntax, see Cisco Express Forwarding Overview and Configuring Cisco Express Forwarding.
Step 3	Router(config)#**interface FastEthernet** *slot/port*	Enters FastEthernet interface configuration mode.
Step 4	Router(config-if)#**ip address** *ip-address mask*	Defines the primary IP address range for the interface.
Step 5	Router(config-if)#**mpls ip**	Enables the interface to be forwarded to an MPLS packet.
Step 6	Router(config-if)#**exit**	Returns to global configuration mode.
Step 7	Router(config)#**mpls label-protocol ldp**	Enables Label Distribution Protocol (LDP). For information about LDP and MPLS, see Configuring Multiprotocol Label Switching.

	Command or Action	Purpose
Step 8	Router(config)# **exit**	Returns to the configuration mode.

Verifying the MPLS VPN Configuration

Use the following commands to verify MPLS VPN operations on PE routers. For more MPLS VPN verification commands, see Configuring Multiprotocol Label Switching.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show ip vrf**	Displays the set of VRFs and interfaces.
Step 2	Router# **show ip route vrf [vrf-name]**	Displays the IP routing table for a VRF.
Step 3	Router# **show ip protocols vrf [vrf-name]**	Displays the routing protocol information for a VRF.
Step 4	Router# **show ip route vrf** *vrf-name*	Displays the Local and Remote CE devices that are in the PE routing table.
Step 5	Router# **show mpls forwarding-table**	Displays entries for a VPN Routing/Forwarding instance.

What to Do Next

For more verification instructions, see the MPLS: Layer 3 VPNs Configuration Guide.

Configuration Examples

This section provides the following configuration examples:

Subinterface Configuration Example

The following example shows how to define a subinterface on virtual bundle interface 1.

```
interface cable3/0
! No IP address
! MAC level configuration only
! first subinterface
interface bundle1.1
description Management Subinterface
ip address 10.255.1.1 255.255.255.0
cable helper-address 10.151.129.2
! second subinterface
interface bundle1.2
ip address 10.279.4.2 255.255.255.0
cable helper-address 10.151.129.2
```

```
! third subinterface
interface bundle1.3
ip address 10.254.5.2 255.255.255.0
cable helper-address 10.151.129.2
```

Cable Interface Bundling Example

The following example shows how to bundle a group of physical interfaces.

interface cable 3/0 and interface cable 4/0 are bundled.

```
interface cable 3/0
 cable bundle 1
interface cable 4/0
 cable bundle 1
interface Bundle 1
 ip address 209.165.200.225 255.255.255.0
 ip address 209.165.201.1 255.255.255.0 secondary
```

Subinterface Definition on Virtual Bundle Example

The following example shows how to define subinterfaces on a virtual bundle and define Layer 3 configurations for each subinterface.

interface cable 3/0 and interface cable 4/0 are bundled.

```
interface cable 3/0
! No IP address
! MAC level configuration only
cable bundle 1
interface cable 4/0
! No IP address
! MAC layer configuration
cable bundle 1
! first subinterface
interface bundle1.1
ip address 10.22.64.1 255.255.255.0
cable helper-address 10.4.1.2
! second subinterface
interface bundle1.2
ip address 10.12.39.1 255.255.255.0
cable helper-address 10.4.1.2
! third subinterface
interface bundle1.3
ip address 10.96.3.1 255.255.255.0
cable helper-address 10.4.1.2
```

Cable Interface Bundle Master Configuration Example

The following examples show how to configure cable interface bundles:

```
Displaying the contents of the bundle
Router(config-if)#cable bundle ?
  <1-255>  Bundle number
Router(config-if)#cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

PE Router Configuration Example

```
!
! Identifies the version of Cisco IOS software installed.
version 12.0
! Defines the hostname of the Cisco uBR7246
hostname region-1-ubr
!
! Describes where the system is getting the software image it is running. In
! this configuration example, the system is loading a Cisco uBR7246 image named
! AdamSpecial from slot 0.
boot system flash slot0:ubr7200-p-mz.AdamSpecial
!
! Creates the enable secret password.
enable secret xxxx
enable password xxxx
!
! Sets QoS per modem for the cable plant.
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
! Allows the system to use a full range of IP addresses, including subnet zero, for
! interface addresses and routing updates.
ip subnet-zero
!
! Enables Cisco Express Forwarding.
ip cef
!
! Configures a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to insert the
! DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information option
!
! Enters the virtual routing forwarding (VRF) configuration mode and maps a VRF table to
! the virtual private network (VPN) called MGMT-VPN. The VRF table contains the set of
! routes that points to or gives routes to the CNR device, which provisions the cable
! modem devices. Each VRF table defines a path through the MPLS cloud.
ip vrf MGMT-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:1
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target export 100:2
 route-target export 100:3
!
! Maps a VRF table to the VPN called ISP1-VPN.
ip vrf ISP1-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:2
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target import 100:1
!
! Maps a VRF table to the VPN called ISP2-VPN.
ip vrf ISP2-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:3
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target import 100:1
!
! Maps a VRF table to the VPN called MSO-isp. Note: MSO-isp could be considered ISP-3; in
! this case, the MSO is competing with other ISPs for other ISP services.
ip vrf MSO-isp
```

```
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:4
!
! Creates a list of import and/or export route target communities for the VPN.
  route-target import 100:1
!
! Builds a loopback interface to be used with MPLS and BGP; creating a loopback interface
! eliminates unnecessary updates (caused by physical interfaces going up and down) from
! flooding the network.
interface Loopback0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
!
! Assigns an IP address to this Fast Ethernet interface. MPLS lable protocol must be
! enabled on this interface.
interface FastEthernet0/0
 description Connection to MSO core.
 ip address 10.0.1.1 255.255.255.0
 no ip directed-broadcast
 full-duplex
 mpls ip
 mpls label protocol ldp
!
! Enters cable interface configuration mode and configures the physical aspects of the
! 3/0 cable interface. Please note that no IP addresses are assigned to this interface;
! they will be assigned instead to the logical subinterfaces. All other commands for
! this cable interface should be configured to meet the specific needs of your cable RF
! plant and cable network.
interface Cable3/0
 no ip address
 cable bundle 1
 ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 855000000
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
!
! Configures bundle 1.1 subinterface. If cable modems have
! not been assigned IP addresses, they will automatically come on-line using the settings
! for subinterface bundle1.1.
interface bundle1.1
 description Cable Administration Network
!
! Associates this interface with the VRF and MPLS VPNs that connect to the MSO cable
! network registrar (CNR). The CNR provides cable modems with IP addresses and other
! initialization parameters.
 ip vrf forwarding MSO
!
! Defines a range of IP addresses and masks to be assigned to cable modems not yet associated
 with an ISP.
 ip address 10.0.0.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PCs that are not yet associated with an ISP.
```

```
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures bundle1.2 subinterface.
interface bundle1.2
 description MSO as ISP Network
!
! Assigns this subinterface to the MPLS VPN used by the MSO to supply service to
! customers—in this case, MSO-isp.
 ip vrf forwarding MSO-isp
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.1.0.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures bundle1.3 subinterface
interface bundle1.3
 description ISP1's Network
!
! Makes this subinterface a member of the MPLS VPN.
 ip vrf forwarding isp1
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Configures bundle1.4 subinterface
interface bundle1.4
 description ISP2's Network
!
! Makes this subinterface a member of the MPLS VPN.
```

```
 ip vrf forwarding isp2
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.2.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
!
 cable dhcp-giaddr policy
!
!! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
end
```

P Router Configuration Example

```
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R7460-7206-02
!
enable password xxxx
!
ip subnet-zero
ip cef
ip host brios 223.255.254.253
!
interface Loopback0
 ip address 10.2.1.3 255.255.255.0
 no ip directed-broadcast
!
interface Loopback1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 1.7.108.2 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 full-duplex
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/0
 ip address 10.0.5.2 255.255.255.0
```

```
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/1
 ip address 10.0.1.17 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/2
 ip address 10.0.2.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/3
 ip address 10.0.3.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/4
 ip address 10.0.4.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/5
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
 no cdp enable
!
interface Ethernet1/6
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
 no cdp enable
!
interface Ethernet1/7
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
 no cdp enable
!
router ospf 222
 network 10.0.5.0 255.255.255.0 area 0
 network 10.0.2.0 255.255.255.0 area 0
 network 10.0.3.0 255.255.255.0 area 0
 network 10.0.4.0 255.255.255.0 area 0
 network 20.2.1.3 255.255.255.0 area 0
!
ip classless
no ip http server
```

```
!
!
map-list test-b
no cdp run
!
tftp-server slot0:master/120/c7200-p-mz.120-1.4
!
line con 0
 exec-timeout 0 0
 password xxxx
 login
 transport input none
line aux 0
line vty 0 4
 password xxxx
 login
!
no scheduler max-task-time
end
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Cable Command Reference* at http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **cable bundle**
- **cable helper-address**
- **ip dhcp relay information option**
- **show cable bundle**

Additional References

Related Documents

For additional information on the Cisco uBR7200 series and MPLS VPN, see:

- Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide
- Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide
- Cisco uBR7200 Series Software Release Notes and Features
- Cisco uBR7200 Series Configuration Notes
- Cisco Network Registrar for the Cisco uBR7200 Series Universal Broadband Routers
- Regulatory Compliance and Safety Information for the Cisco uBR7200 Series Universal Broadband Router
- Configuring Multiprotocol Label Switching
- MPLS Label Switching on Cisco Routers
- Cisco IOS Release 12.1 Documents

Standards

DOCSIS 1.0.

MIBs

- CISCO-DOCS-REMOTE-QUERY.my

No new or modified MIB objects are supported by the cable interface bundling feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

- RFC 1163, A Border Gateway Protocol
- RFC 1164, Application of the Border Gateway Protocol in the Internet
- RFC 2283, Multiprotocol Extensions for BGP-4
- RFC 2547, BGP/MPLS VPNs
- RFC 2233, DOCSIS OSSI Objects Support
- RFC 2669, Cable Device MIB
- RFC 2665, DOCSIS Ethernet MIB Objects Support

Feature Information for Cisco uBR7200 Series MPLS VPN Cable Enhancements

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Feature Name	Releases	Feature Information
Support for Multiprotocol Label Switching Virtual Private Network (MPLS VPN) and Cable Interface Bundling	12.2(33)SCA	Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers

CHAPTER 36

Generic Routing Encapsulation on the Cisco CMTS Routers

First Published: February 14, 2008

This document describes the Generic Routing Encapsulation (GRE) feature. This feature is a tunneling protocol that enables the encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Generic Routing Encapsulation

- The Cisco uBR7246VXR or Cisco uBR10012 router must be running Cisco IOS 12.3(17a)BC or later release.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) module for use with Generic Routing Encapsulation.
- To use GRE, you must identify the inside interfaces on your devices and specify these in the Router MC Settings configuration area. Inside interfaces are the physical interfaces on the device that connect the device to its internal subnets and networks.
- In Router MC, you must select a routing protocol whenever you enable GRE. The available routing protocols in Router MC are EIGRP and Open Shortest Path First (OSPF):
  - Enhanced Interior Gateway Routing Protocol (EIGRP) allows the exchange of routing information within an autonomous system and addresses some of the more difficult issues associated with routing in large, heterogeneous networks. Compared to other protocols, EIGRP provides superior convergence properties and operating efficiency. EIGRP combines the advantages of several different protocols.
  - OSPF is a link-state, hierarchical protocol that features least-cost routing, multipath routing, and load balancing.

Note Do not configure OSPF on the port channel member interface because the OSPF configuration on this interface might cause abnormal behavior of the port channel.

- In Router MC, you must specify an Interior Gateway Protocol (IGP) process number. This number identifies the IGP. When GRE is implemented, this IGP will be the secured IGP. See How Does Router MC Implement GRE? for more information about IGPs. For secure communication, the inside interfaces on peering devices in your VPN must belong to the same IGP. The IGP process number must be within the range specified in the configuration support settings under the Admin tab. If you have an existing IGP on the device that is within this range, but is different from the IGP process number specified in your GRE settings, Router MC will remove the existing IGP. If the existing IGP process number matches the one specified in your GRE settings, any networks included in the existing IGP process that do not match the specified inside interfaces, will be removed.
- If the inside interfaces on your devices are configured to use an IGP other than the IGP specified in your GRE settings (meaning that the interfaces belong to an unsecured IGP):
  - For spokes: Manually remove the inside interfaces from the unsecured IGP by means of the device CLI before configuring GRE with Router MC.

    - For hubs: If the hub inside interface is used as a network access point for Router MC, then on deployment, the interface will be published in both secured and unsecured IGPs. To ensure that the spoke peers use only the secured IGP, manually add the auto-summary command for the unsecured IGP or remove the unsecured IGP for that inside interface.

- In Router MC, you must provide a subnet that is unique and not globally-routable for loopback. This subnet must only be used to support the implementation of loopback for GRE. The loopback interfaces are created, maintained, and used only by Router MC. You should not use them for any other purpose.
- If you are using static routes instead of unsecured IGP, make sure you configure static routes on the spokes through to the hub inside interfaces

Important Notes about Configuring GRE

- You can define GRE on the Global object or on any device group (with the exception of a High Availability (HA) group).
- You can define different GRE policies for different groups of devices within your hierarchy. If you define GRE on Global, the GRE settings will be inherited by all device groups and devices in the hierarchy. You can override the Global GRE policy by defining a different GRE policy on one or more device groups.
- Peering devices must be configured with the same failover and routing policy. Therefore, if you define a specific GRE policy on a device group, both the hub and the spoke must be descendants of that device group and there must be no overriding policy on a lower level that changes the GRE policy on either the peering hub or spoke.
- Switching from IKE keepalive to GRE—If you previously used IKE keepalive for failover, and you later switch to GRE, everything outside your attached networks will no longer be a part of your VPN. Attached networks include only those networks that are directly connected to the router's inside interfaces.

Restrictions for Generic Routing Encapsulation

- To run GRE configuration, you need to have IP connectivity between the cable modems.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) modules for use with Generic Routing Encapsulation. The GRE feature is not supported for PRE1 modules in the Cisco uBR10012 router.

Information About Generic Routing Encapsulation

To configure the Generic Routing Encapsulation feature, you should understand the following concepts:

Tunneling

Tunneling (also known as port forwarding) is a technique that enables remote access users to connect to a variety of network resources through a public data network. The tunnels established through the public network are usually point-to-point, though a multipoint tunnel is possible, and is use to link a remote user to a resource

at the far end of the tunnel. Major tunneling protocols encapsulate Layer 2 traffic from the remote user and send it across the public network to the far end of the tunnel, where it is de-encapsulated and sent to its destination.

Tunneling requires three different protocols:

- Passenger protocol—The original data (IPX, NetBeui, IP) being carried.
- Encapsulating protocol—The protocol (GRE, IPSec, L2F, PPTP, and L2TP) that is wrapped around the original data.
- Carrier protocol—The protocol used by the network over which the information is traveling.

The original packet (Passenger protocol) is encapsulated inside the encapsulating protocol, which is then put inside the carrier protocol's header (usually IP) for transmission over the public network. Note that the encapsulating protocol also quite often carries out the encryption of the data. As you can see, protocols such as IPX and NetBeui, which would normally not be transferred across the Internet, can safely and securely be transmitted.

For site-to-site virtual private networks (VPNs), the encapsulating protocol is usually IPSec or Generic Routing Encapsulation (GRE). GRE includes information on what type of packet you are encapsulating and information about the connection between the client and server.

For remote-access VPNs, tunneling normally takes place using Point-to-Point Protocol (PPP). Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. PPP tunneling will use one of PPTP, L2TP or Cisco's Layer 2 Forwarding (L2F).

The most significant benefit of Tunneling is that it allows for the creation of VPNs over public data networks to provide cost savings for both end users, who do not have to create dedicated networks, and for Service Providers, who can leverage their network investments across many VPN customers.

Generic Routing Encapsulation Overview

GRE Tunneling is a protocol for transporting an arbitrary network layer protocol (the payload) over another arbitrary network layer protocol (the delivery). This is achieved by encapsulating the payload packet in a delivery packet, along with a GRE header. By having both protocols encapsulate IP packets within an additional outer IP header, this enables the transport of IP multicast IP packets across a unicast-only backbone.

The following are some of the advantages of GRE tunnels:

- GRE tunnels provide multi-protocol local networks over a single-protocol backbone.
- GRE tunnels provide workarounds for networks that contain protocols with limited hop counts.
- GRE tunnels connect discontinuous sub-networks.
- GRE tunnels allow VPNs across WANs.

How to Configure Generic Routing Encapsulation

Use the following procedures to configure the GRE feature.

Before configuring the GRE feature:

- Please read the following topics:

◦ Prerequisites for Generic Routing Encapsulation, on page 966

◦ Important Notes about Configuring GRE, on page 967

• If workflow mode is enabled, make sure that you are working within the context of an open activity.

Step 1 Select Configuration > Settings

Step 2 Select General VPN> Failover and Routing in the TOC. The Failover and Routing page appears. the table describes the elements in the Failover and Routing page.

Step 3 Select GRE in the Policy Type list box.The page refreshes to display only the fields that are relevant for GRE configuration.

Step 4 Enter information in the displayed GRE fields, as required. Click Advanced to display additional GRE fields (optional). See the table for a description of each field.

Step 5 Click Apply.

What to Do Next

Table 99: Failover and Routing: GUI Reference

GUI Element	Description
Policy Type list box	Select the type of failover method you want to use. The page will refresh to display only the fields relevant for your selection. • IKE Keepalive • GRE. • GRE Dynamic IP • DMVPN
GRE Elements	
Routing Protocol list box	Select either EIGRP or OSPF as the routing protocol. See Prerequisites for Configuring and Deploying GRE for more information.
Tunnel Interface IP field	Enter a private IP address, including the subnet mask in bits, which defines a subnet in your enterprise to be used to support the implementation of loopback for GRE. For example, 192.10.9.1/255.255.255.0. Router MC creates a loopback interface on the peering devices, with an IP address from this subnet. The loopback interfaces serve as the GRE tunnel endpoints.

GUI Element	Description
Tunnel Source IP field	For GRE Dynamic IP only. Enter a private IP address, including the subnet mask in bits. **Note** To provide robust, stable tunnels, Router MC creates a static IP route using this IP address. If you change this IP address or you change the failover and routing policy, Router MC does not remove the static route from the device configuration. Please consider this if you have a problem with unstable GRE tunnels.
Enable IP Multicast check box	Select this check box to enable multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth. When IP Multicast is enabled, you must specify a rendezvous point that acts as the meeting place for sources and receivers of multicast data.
Rendezvous Point field	This field is only editable when the IP Multicast check box is selected. Enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.
Allow direct spoke to spoke tunnels check box	For DMVPN only. Select this check box to enable direct communication between spokes, without going through the hub. **Note** Note With direct spoke-to-spoke communication, you must use the Main Mode Address option for preshared key negotiation.
Advanced or Basic button	Click the Advanced button to display additional fields for optional advanced configuration. Router MC provides default values for all the advanced options. You can change these default values if required. When the advanced fields are displayed, click the Basic button to display only the basic configuration fields and hide the advanced fields.

GUI Element	Description
Process Number field	Router MC adds an additional Interior Gateway Protocol (IGP) that is dedicated for IPSec and GRE secured communication. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol, either EIGRP or OSPF. Each “routing group” is identified by a logical number, the process number. Enter a routing process number that will be used to identify the secured IGP that Router MC adds when configuring GRE. The number that you provide must be within the range specified next to the field name. The default is the lowest value in the range. This range can be changed in the Configuration Support Settings page in the Admin tab.
Delay	Specify the throughput delay for the interface, in seconds.
Hello Interval EIGRP	Specify the interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time EIGRP	Specify the number of seconds the router will wait to receive a hello message before invalidating the connection. The default hold time is 15 seconds (three times the hello interval).
Tunnel Key field	For DMVPN only. Enter a number that identifies the tunnel key. The tunnel key differentiates between different multipoint GRE (mGRE) tunnel Non Broadcast Multiple Access (NBMA) networks. All mGRE interfaces in the same NBMA network must use the same tunnel key value. If there are two mGRE interfaces on the same router, they must have different tunnel key values.
Network ID (NHRP) field	For DMVPN only. All NHRP stations within one logical NBMA network must be configured with the same network identifier. Enter a globally unique, 32-bit network identifier within the range of 1 to 4294967295.
Hold Time (NHRP) field	For DMVPN only. Enter the time in seconds that routers will keep information provided in authoritative Next Hop Resolution Protocol (NHRP) responses. The cached IP-to-NBMA (non-broadcast multi-access) address mapping entries are discarded after the hold time expires. The default is 600 seconds.
Authentication (NHRP) field	For DMVPN only. Enter an authentication string that controls whether the source and destination NHRP stations allow intercommunication. All routers within the same network using NHRP must share the same authentication string. The string can be up to eight characters long.
Apply button	Click to apply your definitions.

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Additional References

The following sections provide references related to the GRE feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco CMTS Cable Command Reference, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Configuring GRE Tunnel over Cable	Configuring GRE Tunnel over Cable, at the following URL: http://www.cisco.com/en/US/tech/tk86/tk89/technologies_configuration_example09186a008011520d.shtml

Standards

Standard	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 1701	Generic Routing Encapsulation (GRE)
RFC 1702	Generic Routing Encapsulation over IPv4 networks
RFC 1853	IP in IP Tunneling
RFC 2003	IP Encapsulation within IP
RFC 2784	Generic Routing Ecapsulation (GRE)
RFC 2890	Key and Sequence Number Extensions to GRE

Technical Assistance

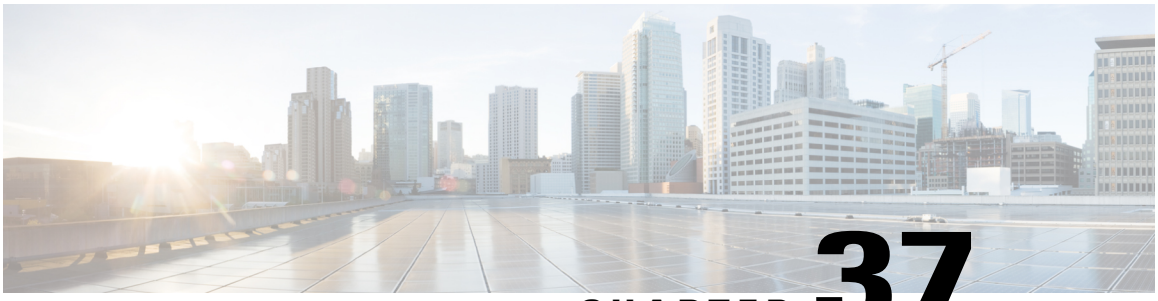
Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Generic Routing Encapsulation

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Feature Name	Release	Feature Information
Generic Routing Encapsulation	12.2(33)SCA	Generic Routing Encapsulation (GRE) is a tunneling protocol that enables the encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers.



CHAPTER 37

L2VPN Support over Cable

First Published: February 14, 2008

Last Updated: January 26, 2012

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

In Cisco IOS Release 12.2(33)SCA, the Layer 2 VPN (L2VPN) Support over Cable feature on the Cisco CMTS provides point-to-point Transparent LAN Service (TLS) in support of the Business Services over DOCSIS (BSOD) CableLabs specification.

The L2VPN Support over Cable feature in Cisco IOS Release 12.2(33)SCA differs from prior L2VPN and TLS support for cable in Cisco IOS release 12.3BC in the following ways:

- Both features use an Ethernet trunking interface to transport traffic for multiple L2VPN tunnels in support of different cable modems (CMs) and service flows (SFs) based on IEEE 802.1q VLAN IDs. For the the legacy TLS service, only the primary upstream or downstream SFs are used. With the new L2VPN Support over Cable feature, both primary and secondary SFs can be used.
- The TLS feature uses CLI to provision the service. The L2VPN Support over Cable feature uses the CM configuration file to provision the service, and a single CLI to identify the default Ethernet Network System Interface (NSI).
- Downstream traffic is forwarded on a per-CM basis and upstream traffic is forwarded on a per-SF basis. For L2VPN Support over Cable feature, upstream traffic for the same L2VPN can use multiple upstream service flows and downstream traffic can use different downstream service flows.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for L2VPN Support over Cable

- You should use crypto-supported images. Refer to the Release Notes for Cisco Universal Broadband Routers in Cisco IOS Release 12.2SC for the latest image information.
- Cable modems must be configured to support BPI+.

This table shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 100: L2VPN Support over Cable Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [60]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [61]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V

60 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

61 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for L2VPN Support over Cable

The L2VPN Support over Cable feature has the following general restrictions:

- DOCSIS 1.0 CMs are not supported.
- Load balancing and Dynamic Channel Change (DCC) are not supported for CMs that are enabled for L2VPN support.
- DSx messages (Dynamic Service Add [DSA], Dynamic Service Change [DSC], and Dynamic Service Delete [DSD]) are supported for L2VPN-provisioned CMs from Cisco IOS Release 12.2(33)SCF2 onwards. However, DSx with L2VPN type, length, values (TLVs) are not supported.
- Multipoint L2VPN is not supported, and any Simple Network Management Protocol (SNMP) MIBs for multipoint L2VPN are not supported.
- eSAFE (embedded Service/Application Functional Entities) DHCP snooping is not supported (L2VPN subtype 43.5.3)
- Maximum of 1024 L2VPNs are supported on a single MAC domain.
- Maximum of eight upstream SFs are supported per L2VPN service.
- Maximum of eight downstream classifiers are supported per L2VPN service.

- eSAFE exclusion is supported for only one eSAFE host. If the REG-REQ message for a compliant CM specifies multiple eSAFE hosts, then the eMTA (ifIndex 16) is selected as the eSAFE host to be excluded by the Cisco CMTS router. If the eMTA is not included as part of the capability of the CM, then the first eSAFE host in the capability is selected for exclusion.
- Maximum length of the Cable Modem Interface Mask (CMIM) is 4 bytes.
- Areas of the Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks specification that are not supported are:
  - Vendor-specific L2VPN encodings for the replacement of the required VPN ID and NSI Encapsulation subtype are not supported.
  - Mapping of egress user priority to an NSI port transmission traffic class as specified by IEEE 802.1s is not supported.
  - Forwarding with non-zero default user priority values with vendor-specific configuration is not supported.
  - Accepting multiple Downstream Classifier L2VPN Encoding with the same VPN ID to clasify packets to different service flows is not supported.
  - Assigning multiple SAIDs to the same L2VPN on the same CM is not supported. The primary SAID is used for encrypting all downstream traffic.
  - Assigning of the same group-level L2VPN SAID to different CMs on the same MAC domain attached to the same L2VPN identifier is not supported.
  - Implementing the DOCSIS Spanning Tree Protocol (DSTP) and transmission of DSTP BPDUs on all NSI and RF interfaces configured for L2VPN operation is not supported.
  - Implementing a DSTP SAID specifically for DSTP forwarding to the customer premises equipment (CPE) ports of all L2VPN CMs is not supported.

VPN ID Restrictions

- A maximum of four VPN IDs are supported for each CM.
- A maximum of one VPN ID can be associated with each SF in a CM; although multiple SFs in a CM can belong to the same L2VPN.
- A maximum of 4093 unique VPN IDs are supported per Cisco CMTS router.
- The maximum length of a VPN ID is 16 bytes.
- All L2VPN encodings must contain a VPN ID, except for upstream classifier encodings.

Information About L2VPN Support over Cable

L2VPN Support Over Cable provides the following benefits and functions on a Cisco CMTS router:

- Supports point-to-point L2VPN forwarding mode.
- Supports up to four VPN IDs per CM.
- Supports multiple upstream SFs per CM, with one or more SFs belonging to the same VPN ID.

- Supports a single Ethernet NSI that serves as a trunking port for one or more L2VPN tunnels on the Cisco CMTS router.
- Supports BPI+ encryption using primary SAID of the CM.
- Supports L2VPN encodings in the CM configuration file and CM registration (REG-REQ with L2VPN encoding).
- Supports upstream L2VPN tunnel in support of per-CM and per-SF forwarding.
- Supports synchronization and recovery of the L2VPN database and upstream and downstream SFs during PRE2 NSF/SSO and N+1 line card redundancy switchovers.
- Supports QoS in upstream and downstream.
- Supports stacked IEEE 802.1q tags.
- Supports exclusion of traffic from the L2VPN tunnel for a single Embedded Service/Application Functional Entity (eSAFE) host.
- Supports Layer 2 classifier via CMIM and IEEE 802.1p priority bits.
- Supports detection of provisioning errors, such as duplicate VLAN IDs across CMs or existing VLAN IDs in use, and moves a CM offline with a corresponding error message.
- Supports coexistence of L2VPN and non-L2VPN traffic on the same RF MAC domain, with non-L2VPN traffic isolated from other tunnel traffic.
- Supports voice calls from L2VPN-provisioned CMs. However, voice calls are not part of the L2VPN.
- Supports BSOD VLAN Redundancy feature, which allows users to configure a backup WAN interface in addition to the primary WAN interface. When the primary WAN interface is down, the L2VPN traffic flows through the backup WAN interface.
- Supports manual switchover for VLAN Redundancy feature, which allows users to manually switch active uplink port from the current port to another port when both the uplink ports are up.

Point-to-Point L2VPN Forwarding Mode

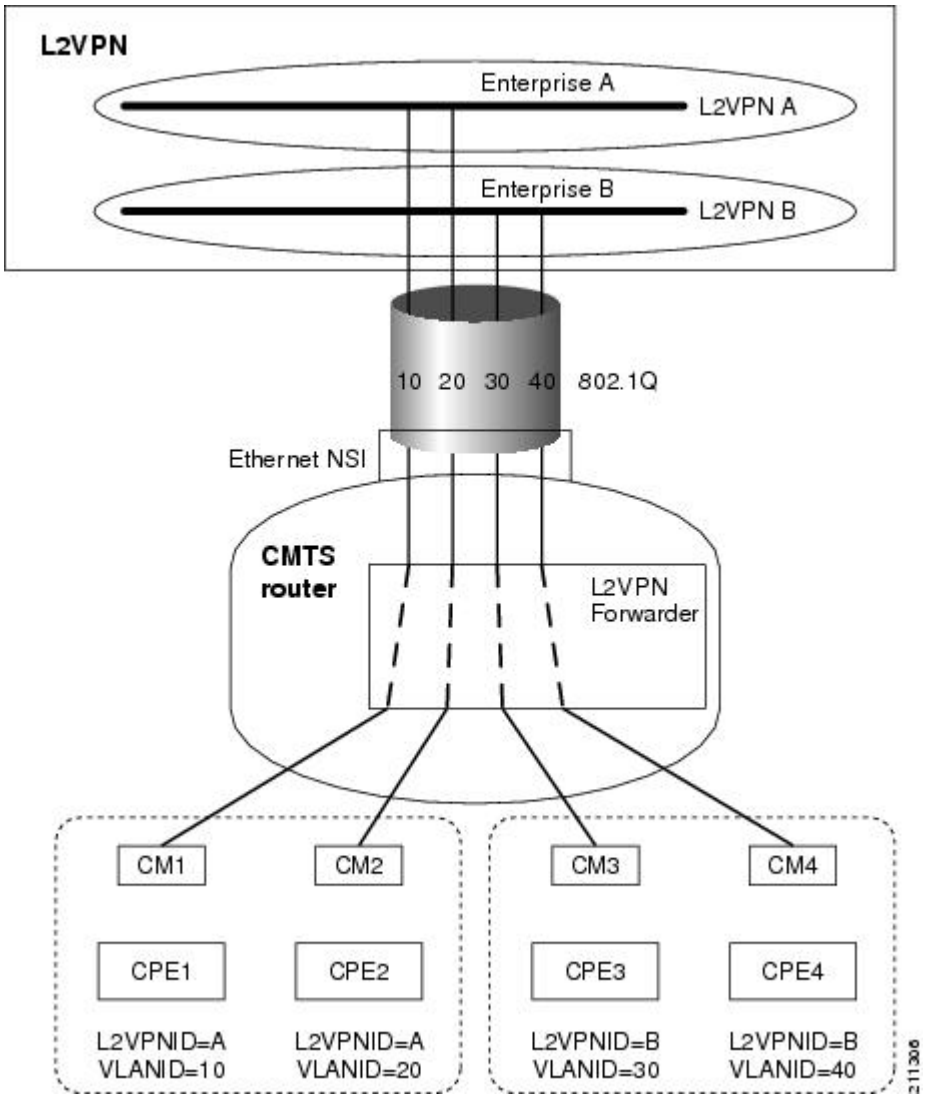
The Cisco CMTS routers in Cisco IOS Release 12.2(33)SCA support the point-to-point L2VPN forwarding mode described in the BSOD specification. Each attachment circuit (either SF or CM) on the Cisco CMTS router has a NSI encapsulation value, and is configured with an IEEE 802.1q VLAN ID.

The L2VPN forwarder on the Cisco CMTS router forwards both upstream and downstream traffic between the NSI port on the router and an attachment circuit without using MAC address learning for the forwarding decision. A L2VPN bridge on the backbone network of the cable operator performs the MAC-address learning to bridge packets between VLAN IDs.

The image below shows an example of a point-to-point L2VPN network using IEEE 802.1q NSI encapsulation. In this example, four CMs are associated with four different VLAN IDs: 10, 20, 30, and 40. The L2VPN

encoding of the CM includes the logical L2VPN ID (in this case, A or B) with an NSI encapsulation subtype for IEEE 802.1q with the associated VLAN ID.

Figure 23: Point-to-Point L2VPN Network Diagram



The logical L2VPN IDs allow creation of separate broadcast domains for certain VLAN IDs. In the diagram, traffic for VLANs 10 and 20 from CM1 and CM2 can be sent to the network of Enterprise A, and traffic for VLAN's 30 and 40 from CM3 and CM4 can be sent to the network of Enterprise B.

L2VPN Encodings in the CM Configuration File

The CM configuration file contains a set of L2VPN encodings that control how the Cisco CMTS processes L2VPN forwarding of upstream and downstream CPE packets. As per the BSOD specification, the L2VPN encoding is encapsulated using a General Extension Information (GEI) encoding, which uses the type code 43 and subtype of 5 (43.5) with the reserved Vendor ID of 0xFFFFFF.

L2VPN defines the following types of encodings:

- Per-CM L2VPN encodings—An encoding that appears at the top level of the CM configuration file.
- Per-SF L2VPN Encoding—An encoding that appears as a subtype of the Upstream Service Flow Encoding (type 24).
- Upstream Classifier L2VPN Encoding—An encoding that appears in an Upstream Packet Classification Configuration Setting (type 22).
- Downstream Classifier L2VPN Encoding—An encoding that appears in a Downstream Packet Classification Configuration Setting (type 23).

The simplest CM configuration file has a single per-SF L2VPN Encoding within the primary upstream SF definition and a single per-CM L2VPN Encoding with a NSI Encapsulation subtype for that L2VPN.

Note When BSOD (CM configuration file) is used for L2VPN configuration, and QoS policy-map settings are applied to Cisco CMTS WAN interfaces, the packets do not match the QoS policy-map. When CLI mode is used for L2VPN configuration, and QoS policy-map settings are applied to Cisco CMTS WAN interfaces, the packets will match the QoS policy-map first.

Note Starting from Cisco IOS 12.2(33)SCJ release, CMTS supports BSOD VLAN redundancy feature with support for two Ethernet Network Side Interface (NSI) configuration and a backup WAN interface. When the active NSI WAN interface is down, the L2VPN traffic flows through the backup WAN interface.

Supported L2VPN Encodings

This section describes the supported L2VPN encodings in the CM configuration file that are supported by the Cisco CMTS routers.

- The Cisco CMTS routers support the following CM capabilities:
  - L2VPN capability (5.17)
  - eSAFE host capability (5.18)
  - Downstream Unencrypted Traffic (DUT) filtering (5.19)
- The Cisco CMTS routers support the following top-level encodings:
  - VPN identifier (43.5.1)
  - CMIM (43.5.4)—When provided, applies to all upstream SFs associated with an L2VPN tunnel; Supports only one eSAFE host.
  - NSI encapsulation (43.5.2) with format code 2 for IEEE 802.1q (43.5.2.2)
  - DUT filtering encoding
- The Cisco CMTS routers support the following per-SF encodings:
  - VPN identifier (43.5.1)
  - Ingress user priority (43.5.8)

- The Cisco CMTS routers support the following downstream classifier encodings:
  - VPN identifier (43.5.1)
  - CMIM (43.5.4) and (22/23.13)
  - User priority range (43.5.9)

For more information about the CM configuration file and L2VPN encodings, see the "Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks" specification.

For information about how to use the configuration file generator on the Cisco CMTS, see the “DOCSIS Internal Configuration File Generator for the Cisco CMTS” document.

SNMPv3 Interface

L2VPN Support over Cable in Cisco IOS Release 12.2(33)SCA supports the following MIBs in SNMPv3:

- DOCSIS-L2VPN-MIB

For a link to the Cisco IOS MIB tools, see the http://tools.cisco.com/ITDIT/MIBS/servlet/index.

DOCSIS-L2VPN-MIB

The DOCSIS-L2VPN-MIB contains the SNMP management objects used by the Cisco CMTS router for L2VPN support. The MIB is bundled with the Cisco IOS software images that support the L2VPN Support over Cable feature.

Table 101: DOCSIS-L2VPN-MIB Tables , on page 982 lists the tables in the DOCSIS-L2VPN-MIB supported by the Cisco CMTS routers. For more information, see the MIB documentation.

Table 101: DOCSIS-L2VPN-MIB Tables

Object	Description
docsL2vpnIdToIndexTable	Indexed by the octet string DocsL2vpnIdentifier that provides the local agent's internally assigned docsL2vpnIdx value for that DocsL2vpnIdentifier value.
docsL2vpnIndexToIdTable	Indexed by agent's local docsL2vpnIdx that provides the global L2VPN Identifier.
docsL2vpnCmTable	Describes L2VPN per-CM information that is in common with all L2VPNs for the CM, regardless of forwarding mode.
docsL2vpnVpnCmTable	Describes the operation of L2VPN forwarding on each CM.
docsL2vpnVpnCmStatsTable	Contains statistics for forwarding of packets to and from a CM on each VPN.

Object	Description
docsL2vpnPortStatusTable	Displays summary information for the run-time state of each VPN that is currently operating on each bridge port.
docsL2vpnSfStatusTable	Displays SF-specific L2VPN forwarding status for each upstream service flow configured with a per-SF L2VPN encoding.
docsL2vpnPktClassTable	Provides the L2VPN-specific objects for packet classifiers that apply to only L2VPN traffic. The indices of this table are a subset of the indices of classifiers in the docsQosPktClassTable.
docsL2vpnCmNsiTable	Describes the NSI configuration for a single CM when operating in point-to-point forwarding mode for an L2VPN.

Voice-Call Support on L2VPN CM

Cisco IOS Release 12.2(33)SCF2 introduces the Voice-Call Support on L2VPN CM feature. This feature enables the Cisco CMTS routers to support dynamic service flows on L2VPN-provisioned cable modems to permit voice calls from a non-L2VPN CPE.

To provide voice-call support on a L2VPN CM, you have to configure correct classifiers and create two static service flows (primary and secondary) using the cable modem configuration file. If the eMTA is L2VPN-capable with the embedded CPE configured as an eSAFE host, then only one service flow is required. When correct CMIM bits are configured, the Cisco CMTS does not send packets from the eSAFE host to the L2VPN.

Though the L2VPN can be configured on the primary or secondary service flow, it cannot coexist with eMTAs on the same service flow. The eMTAs should always use a different service flow from that of L2VPN. The classifiers to direct the traffic should also be based on the service flows the L2VPN and eMTAs are using. When the above configuration is in place, the dynamic service flows are created automatically whenever voice calls are initiated.

How to Configure L2VPN Support over Cable

This section contains the following procedures:

Configuring the Ethernet Network System Interface

To configure the L2VPN Support over Cable feature, you need to specify an Ethernet NSI to operate as the trunking interface for the L2VPN traffic. You must configure the NSI using a command on the Cisco CMTS router. It is not configurable through the CM configuration file.

Before You Begin

The following interface types can be configured as an NSI for L2VPN Support over Cable:

- Cisco uBR10012 Universal Broadband Router—Gigabit Ethernet.
- Cisco uBR7246VXR Universal Broadband Router—Fast Ethernet or Gigabit Ethernet

Note The Cisco CMTS routers only support the configuration of a single L2VPN NSI per CMTS.

>

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2-vpn-service xconnect nsi dot1q interface***ethernet-intf***[backup-interface ethernet-intf]** **Example:** `Router(config)# cable l2-vpn-service xconnect nsi dot1q interface Te4/1/0 backup-interface Te4/1/4`	Configures WAN interface for DOT1Q L2VPN . (Optional) Backup-interface - If backup-interface is configured it means that BSoD VLAN redundancy feature is enabled.

Preparing the DOCSIS Configuration File for L2VPN Support

To support L2VPN, the DOCSIS configuration file must be configured with the appropriate encodings. For information about the supported encodings by the Cisco CMTS routers, see the L2VPN Encodings in the CM Configuration File, on page 980.

Manual Switchover Command Line Interface

For BSoD VLAN Redundancy feature, users can manually switch active uplink ports from the active port to another port when both the uplink ports are up through the command line interface. To manually switchover, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **cable l2-vpn dot1q-nsi-redundancy force-switchover from** *active-nsi-interface*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted
Step 2	**cable l2-vpn dot1q-nsi-redundancy force-switchover from** *active-nsi-interface* **Example:** `Router# cable l2-vpn dot1q-nsi-redundancy force-switchover from Te4/0/1`	Switches the active uplink port from the current active port to the specified port.

To display the dot1q L2VPN uplink redundancy information, use the **show cable l2-vpn dot1q-nsi-redundancy** as shown in the following example:

```
Router# show cable l2-vpn dot1q-nsi-redundancy
Primary-NSI Backup-NSI Active-NSI Elapsed-after-SW
Te4/1/0       Te4/0/4    Te4/1/0    31m9s
Te4/1/2       Te4/0/5    Te4/1/2    59s
```

Verifying L2VPN Support over Cable

To verify L2VPN information on the Cisco CMTS router, use the **show cable l2-vpn xconnect dot1q-vc-map** command.

SUMMARY STEPS

1. To display VLAN information for all cable modems, use the **show cable l2-vpn xconnect dot1q-vc-map** command as shown in the following example:
2. To display VLAN information for a particular L2VPN ID or customer, use the **show cable l2-vpn xconnect dot1q-vc-map customer** form of the command as shown in the following example:
3. To display information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn xconnect dot1q-vc-map vpn** form of the command along with specification of the cable modem MAC address, as shown in the following example:
4. To display detailed information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn xconnect dot1q-vc-map vpn verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:
5. To display detailed information and the current redundancy information for a particular cable modem, use the the **show cable l2-vpn xconnect dot1q-vc-map verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:
6. To display the dot1q L2VPN uplink redundancy information, use the **show cable l2-vpn dot1q-nsi-redundancy** as shown in the following example:

DETAILED STEPS

Step 1 To display VLAN information for all cable modems, use the **show cable l2-vpn xconnect dot1q-vc-map** command as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q-vc-map
MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPN ID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 2 To display VLAN information for a particular L2VPN ID or customer, use the **show cable l2-vpn xconnect dot1q-vc-map customer** form of the command as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q-vc-map customer 0234560001

MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 3 To display information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn xconnect dot1q-vc-map vpn** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001

MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 4 To display detailed information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn xconnect dot1q-vc-map vpn verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001 verbose
MAC Address                    : 0014.f8c1.fd66
Prim Sid                       : 3
Cable Interface                : Cable6/0/0
VPN ID                         : 0234560001
L2VPN SAID                     : 12294
Upstream SFID                  : 23
Downstream CFRID[SFID]         : 2[24]
CMIM                           : 0x60
Ethernet Interface             : GigabitEthernet4/0/0
DOT1Q VLAN ID                  : 68
Total US pkts                  : 1372
Total US bytes                 : 500226
Total US pkt Discards          : 0
Total US byte Discards         : 0
Total DS pkts                  : 1248
Total DS bytes                 : 415584
Total DS pkt Discards          : 0
Total DS byte Discards         : 0
```

Step 5 To display detailed information and the current redundancy information for a particular cable modem, use the the **show cable l2-vpn xconnect dot1q-vc-map verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 verbose
MAC Address                          : 5039.5589.4302
Prim Sid                             : 45
Cable Interface                      : Cable6/0/2
L2VPNs provisioned                   : 1
DUT Control/CMIM                     : Disable/0x8000FFFF

VPN ID                               : 000234560001
L2VPN SAID                           : 45
Upstream SFID Summary                : 77
Upstream SFID [77   ]                : SID 45
Downstream CFRID[SFID] Summary       : Primary SF
CMIM                                 : 0x60
Primary Ethernet Interface           : GigabitEthernet4/0/0
Backup  Ethernet Interface           : GigabitEthernet4/0/1
Active  Ethernet Interface           : GigabitEthernet4/0/0
DOT1Q VLAN ID                        : 207
Total US pkts                        : 151269
Total US bytes                       : 211755224
Total DS pkts                        : 150502
Total DS bytes                       : 210463324
```

Step 6 To display the dot1q L2VPN uplink redundancy information, use the **show cable l2-vpn dot1q-nsi-redundancy** as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-nsi-redundancy
Primary-NSI Backup-NSI Active-NSI Elapsed-after-SW
Te4/1/0       Te4/0/4    Te4/1/0    31m9s
Te4/1/2       Te4/0/5    Te4/1/2    59s
```

Enabling Voice-Call on a L2VPN CM

You can enable the Voice-Call Support on a L2VPN CM feature by registering a cable modem with a SID to VPN mapping cable modem configuration file (MPLS or 802.1q).

- If the L2VPN is on the primary service flow, you should use a cable modem configuration file with static secondary service flow and the classifiers should be configured on the secondary service flow for non-L2VPN packets.
- If the L2VPN is on the secondary service flow, then classifiers should be configured for L2VPN packets.

Note The cable modem configuration file based L2VPN configuration provides the flexibility to configure L2VPN on the primary or secondary service flow. However, we recommend that you configure L2VPN on the secondary service flow and the primary service flow is used for the default traffic.

Note In a CLI-based L2VPN configuration, the L2VPN is on the primary service flow; therefore the static secondary service flow should be used for the eMTAs.

Verifying Dynamic Service Flows

To verify dynamically created service flows on the Cisco CMTS router, use the **show interface cable service-flow** command.

Note To verify information about PacketCable operations, use **show packetcable** commands.

```
Router# show interface cable 5/1/0 service-flow
Sfid : 30191
Mac Address : 000a.739e.140a
Type : Secondary(Dynamic)
Direction : Upstream
Current State : Active
Current QoS Indexes [Prov, Adm, Act] : [0, 24, 24]
Active Time : 00:55
Sid : 7140
Admitted QoS Timeout : 200 seconds
Active QoS Timeout : 0 seconds
Packets : 1824
Bytes : 466944
Rate Limit Delayed Grants : 0
Rate Limit Dropped Grants : 0
Current Throughput : 68356 bits/sec, 32 packets/sec
Classifiers:
Classifier Id : 41
Service Flow Id : 30191
CM Mac Address : 000a.739e.140a
Direction : upstream
Activation State : active
Classifier Matching Priority : 128
PHSI : 1
Number of matches : -
IP Classification Parameters:
IP Source Address : 10.8.230.3
Source IP Address Mask : 255.255.255.255
Destination IP Address : 172.16.2.35
Destination IP Address Mask : 255.255.255.255
IP Protocol Type : 17
Source Port Low : 53456
Source Port High : 53456
Destination Port Low : 7052
Destination Port High : 7052
```

Configuration Examples for L2VPN over Cable

This section provides configuration examples for the L2VPN over Cable feature:

Example: Specifying the Ethernet NSI Interface

You can specify the Ethernet NSI within the CM configuration file, or using the **cable l2-vpn-service xconnect** global configuration command as shown in the following example:

```
cable l2-vpn-service xconnect nsi {dot1q|mpls}
```

Example: Enabling Voice Call Support on MPLS L2VPN

The following is a sample cable modem configuration file that enables voice call support on MPLS L2VPN. In this example the L2VPN is applied to the primary service flow.

```
03 (Net Access Control)          = 1
18 (Maximum Number of CPE)       = 16
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
   S005 (Unknown sub-type)       = 01 04 32 30 32 30 02 07 04 05 01 0a 4c 02 01 2b 06 26 04
 00 00 01 90
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 2
   S03 (Service Flow Reference)          = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)           = 050 001 005 000
       T04 (IP Source Mask)              = 255 255 255 000
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 3
   S03 (Service Flow Reference)          = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)          = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 21
   S03 (Service Flow Reference)          = 21
   S05 (Rule Priority)                   = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)      = 050 001 005 000
       T06 (IP Destination Mask)         = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 22
   S03 (Service Flow Reference)          = 21
   S05 (Rule Priority)                   = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)     = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 1
   S06 (QoS Parameter Set Type)          = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 04 32 30 32 30
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 2
   S06 (QoS Parameter Set Type)          = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 20
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 0
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 21
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 1
29 (Privacy Enable)              = 1
```

Example: Enabling Voice Call Support on 802.1q L2VPN

The following is a sample cable modem configuration file that enables voice call support on 802.1q L2VPN. In this example the L2VPN is applied to the secondary service flow.

```
03 (Net Access Control)          = 1
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
   S005 (Unknown sub-type)       = 01 05 02 34 56 00 01 02 04 02 02 00 44
18 (Maximum Number of CPE)       = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 2
```

```
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 14 e3 23 1c
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 4
   S03 (Service Flow Reference)         = 4
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 07
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01 08 01 01
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 3
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 4
   S06 (QoS Parameter Set Type)         = 7
```

Example: Enabling Voice Call Support on CLI-based L2VPN

The following is a sample cable modem configuration file that enables voice call support on L2VPN configured using CLI. L2VPN configured using the CLI is always applied to the primary service flow.

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)          = 050 001 005 000
       T04 (IP Source Mask)             = 255 255 255 000
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 3
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 21
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)     = 050 001 005 000
       T06 (IP Destination Mask)        = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 22
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)    = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 77
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 20
   S06 (QoS Parameter Set Type)         = 7
   S07 (Traffic Priority)               = 0
25 (Downstream Service Flow Encodings)
```

```
   S01 (Service Flow Reference)          = 21
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 1
29 (Privacy Enable)             = 1
```

Additional References

The following sections provide references related to the L2VPN Support over Cable feature.

Related Documents

Related Topic	Document Title
SNMP configuration information	*Cisco IOS Configuration Fundamentals Configuration Guide,* Part 3: Cisco IOS System Management, "Configuring SNMP Support" section http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html
SNMP command information	*Cisco IOS Network Management Command Reference , Release 12.2SB* http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command/reference/nm_book.html

Standards

Standard	Title
CM-SP-BPI+-I12-050812	*Baseline Privacy Plus Interface Specification* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-BPI+-C01-081104.pdf
CM-SP-L2VPN-I03-061222	*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-L2VPN-I12-131120.pdf
CM-SP-RFIv2.0-I11-060602	*Radio Frequency Interface Specification* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-RFIv2.0-C02-090422.pdf
IEEE 802.1ad	*IEEE 802.1ad-2005 IEEE Standards for Local and metropolitan area networks*— Virtual Bridged Local Area Networks http://www.ieee.org

Standard	Title
IEEE 802.1q	*IEEE Std 802.1Q Virtual Bridged Local Area Networks* http://www.ieee.org

MIBs

MIB	MIBs Link
DOCS-L2VPN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 2685	Virtual Private Networks Identifier http://www.ietf.org/rfc/rfc2685.txt
RFC 4364	*BGP/MPLS IP Virtual Private Networks (VPNs)* http://www.ietf.org/rfc/rfc4364.txt

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for L2VPN Support over Cable

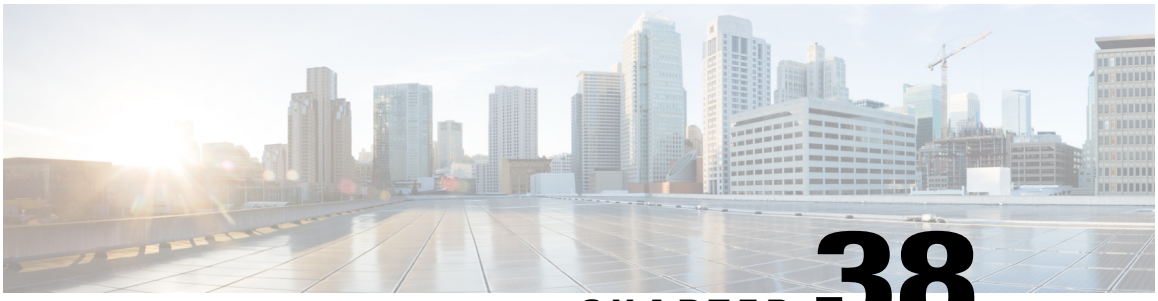
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 102: Feature Information for L2VPN Support Over Cable

Feature Name	Releases	Feature Information
L2VPN Support over Cable	12.2(33)SCA	This feature was introduced and provides point-to-point Transparent LAN Service (TLS) in support of the Business Services over DOCSIS (BSOD) CableLabs specification. The **cable l2-vpn-service default-nsi** command is introduced.
L2VPN Support over Cable	12.2(33)SCC	The **cable l2-vpn-service default-nsi** command is replaced with **cable l2-vpn-service xconnect nsi** {**dot1q** | **mpls**} command.
Voice-Call Support on L2VPN CM	12.2(33)SCF2	This feature allows you to enable voice calls on L2VPN-provisioned cable modem.
BSoD VLAN Redundancy Feature	12.2(33)SCJ	This feature allows you to manually switch active uplink ports.



CHAPTER 38

MPLS Pseudowire for Cable L2VPN

First Published: November 16, 2009

Last Updated: June 20, 2011

The Multiprotocol Label Switching (MPLS) Pseudowire for Cable Layer 2 Virtual Private Network (L2VPN) feature enables service providers to use a single, converged, Internet Protocol (IP)/MPLS network infrastructure to offer Ethernet data link layer (Layer 2) connectivity to two or more VPN customer sites.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

- Feature Information for MPLS Pseudowire for Cable L2VPN, page 1030

Prerequisites for MPLS Pseudowire for Cable L2VPN

- Enable Baseline Privacy Interface Plus (BPI+) to provide a simple data encryption scheme to protect data sent to and from cable modems in a data over cable network.
- Enable Cisco Express Forwarding (CEF) to optimize network performance.
- Ensure that the primary and backup pseudowires on the remote provider edge (PE) routers have the same pseudowire type as the Cisco cable modem termination system (CMTS).
- Create the remote pseudowire using a pw-class with VLAN as the interworking for remote PEs like the c7600, if the CMTS is using VLAN as pseudowire type.

The table shows the CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 103: Hardware Compatibility Matrix for MPLS Pseudowire for Cable L2VPN Feature

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [62]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [63]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

62 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

63 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for MPLS Pseudowire for Cable L2VPN

The following are the general restrictions for the MPLS Pseudowire for Cable L2VPN feature:

- Supports only Ethernet over MPLS (EoMPLS) pseudowires per RFC 4448.
- Supports only point-to-point forwarding. Ethernet switching is not supported.
- Requires DOCSIS 2.0 and 3.0-certified cable modems (CMs). This feature is not supported on DOCSIS 1.0-certified cable modems.
- Supports a maximum of four VPNs per cable modem.
- Supports a maximum of eight upstream service flows and eight downstream classifiers.
- Supports a maximum of 16000 EoMPLS pseudowires per Cisco CMTS router.
- Requires the backup pseudowire to be up on the remote PE for the Cisco CMTS to switchover.
- Requires the backup pseudowire to become active on the Cisco CMTS only after the primary pseudowire fails.

Note The CLI-based (static provisioning) L2VPN supports traffic forwarding to VPN only on primary upstream and downstream service flows. Hence only primary upstream and downstream service flows must be configured in the cable modem configuration file.

Information About MPLS Pseudowire for Cable L2VPN

The MPLS Pseudowire for Cable L2VPN feature enables Ethernet-based Layer 2 VPN service over an MPLS network by encapsulating and transmitting the Layer 2 protocol data units (PDUs) over pseudowires (PWs). This feature enables service providers to offer site-to-site connectivity to their business and enterprise customers.

Layer 2 services emulated over an MPLS network are commonly referred to as MPLS-based L2VPNs or MPLS L2VPNs. Subsequently, Ethernet service emulated over an MPLS network is referred to as Ethernet over MPLS (EoMPLS) service.

The MPLS Pseudowire for Cable L2VPN feature is fully compliant with CableLabs Business Services over DOCSIS (BSOD) L2VPN specification, and is an extension to the existing DOCSIS L2VPN features supported on Cisco CMTS routers.

The MPLS Pseudowire for Cable L2VPN feature provides the following capabilities:

- Transport Ethernet frames over an MPLS network.
- Handle a DOCSIS service flow as an attachment circuit that is mapped to an EoMPLS pseudowire.
- Enable the Cisco CMTS router to be the MPLS provider edge (PE) router.
- Enable forwarding of Ethernet frames over DOCSIS (between a CM and a Cisco CMTS router) to MPLS (towards Metropolitan Area Network or Wide Area Network).
- Provide a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network.

The MPLS Pseudowire for Cable L2VPN feature differs from the existing DOCSIS L2VPN features such as 802.1q-based L2VPN (L2VPN Support over Cable). The MPLS Pseudowire for Cable L2VPN feature uses IP/MPLS network to transport layer 2 protocol data units (PDUs), whereas 802.1q-based L2VPN feature uses layer 2 Ethernet network to transport PDUs.

How MPLS Transports Layer 2 Packets

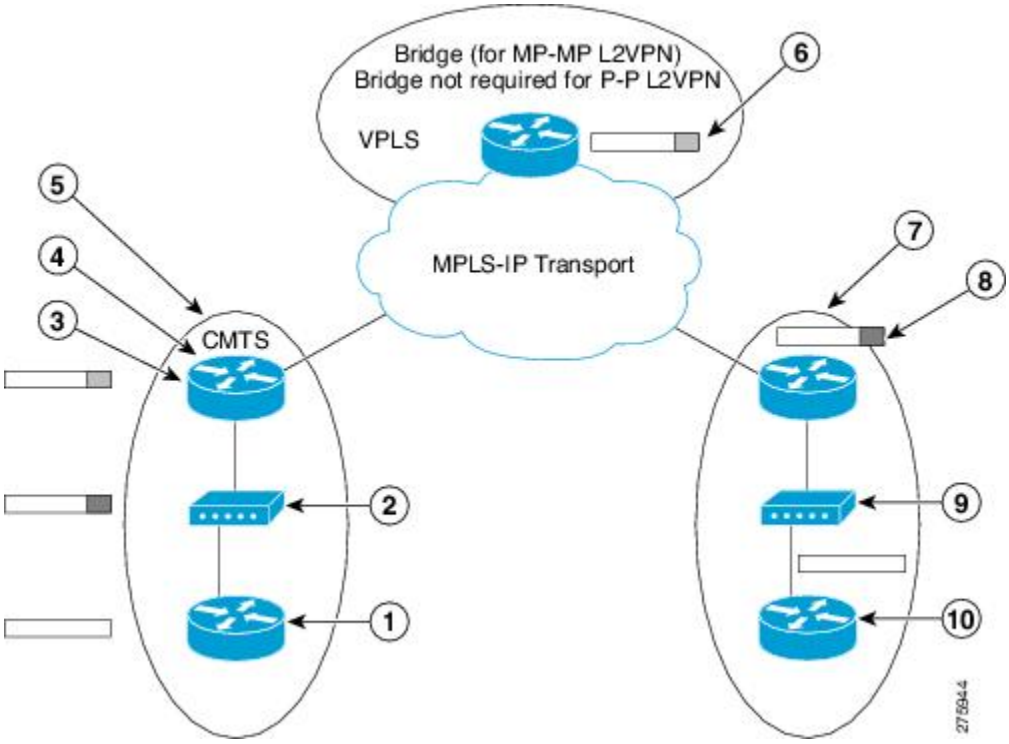
The MPLS subsystem removes DOCSIS encapsulation for Layer 2 Ethernet frames and adds MPLS labels at the ingress provider edge (PE) Cisco CMTS router. Then, the MPLS subsystem sends resulting MPLS packets to the corresponding PE router at the other end of the pseudowire. The PE routers must be configured for successful transmission of IP/MPLS packets between the two PE routers.

The cable modem classifies Ethernet frames from the customer premise equipment (CPE) in the upstream direction using upstream classifiers. Then, a DOCSIS header is added to these frames, and they are sent on a given upstream service flow with a different service identifier. On the Cisco CMTS router, the upstream packet is classified as an L2VPN packet based on the cable interface and service identifier. The Cisco CMTS router removes the DOCSIS header and adds an MPLS header. An MPLS header contains two MPLS labels: the outer label corresponding to the remote PE router and the inner label corresponding to the pseudowire label. The Cisco CMTS router forwards the MPLS packet towards the remote PE router, which is the other end of the pseudowire, over the MPLS network.

In the downstream direction, the Cisco CMTS router receives MPLS packets having only one MPLS header that contains the label that the Cisco CMTS router previously allocated for the corresponding EoMPLS pseudowire. The Cisco CMTS router uses the MPLS label to identify one of the L2VPN cable modems. Then, the Cisco CMTS router classifies the MPLS packet using the L2VPN downstream classifiers based on MPLS experimental (MPLS-EXP) bits in the MPLS header of the received MPLS packet, and removes the MPLS header. Then, the Cisco CMTS router sends the packet on the classified downstream service flow by adding the DOCSIS header. The cable modem then removes the DOCSIS header and delivers the Ethernet frame to the CPE.

A unique combination of a cable modem MAC address, VPN ID (if present in the CM configuration file), peer IP address, and a virtual circuit ID (VCID) identifies the MPLS pseudowire on the Cisco CMTS router.

Figure 24: Transporting Layer 2 Packets



The table illustrates how MPLS transports Layer 2 packets in a DOCSIS-based cable communications system.

1	A router sends an untagged Ethernet frame.	6	MPLS packets are label switched.
2	A CM adds a DOCSIS header to the frame.	7	The Cisco CMTS router receives an MPLS packet and looks up the MPLS forwarding table using the label value in the MPLS header.
3	The Cisco CMTS router removes the DOCSIS header from the frame.	8	The Cisco CMTS router replaces the MPLS header with DOCSIS header (containing the right SID value).

4	The Cisco CMTS router looks up the Service ID (SID) database using the SID value from the DOCSIS header and finds the MPLS header.	9	The DOCSIS header is removed.
5	The Cisco CMTS router adds the MPLS header to the frame.	10	The Ethernet frame is delivered untagged.

Supported Ethernet Encapsulation on UNI

The Ethernet User-Network Interface (UNI) is the connection between a cable modem and a customer premise equipment such as a router or a switch. The service provider may or may not use any encapsulation on the UNI.

The MPLS Pseudowire for Cable L2VPN feature supports the following transport types on an Ethernet UNI:

- Port-based UNI (independent of any VLAN)—The port-based UNI provides Metro Ethernet Forum (MEF)-defined Ethernet Private Line (EPL) service. In this transport type, an MPLS pseudowire is mapped to the Ethernet port.
- VLAN-based UNI—Ethernet VLAN using 802.1q encapsulation (including stacked VLANs). The VLAN-based UNI provides MEF-defined Ethernet Virtual Private Line (EVPL) service. In this transport type, the MPLS pseudowire is mapped to the 802.1q VLAN.

Note The Ethernet UNI must be attached to the Ethernet port of a cable modem.

Before configuring this feature, you should understand the following concepts:

MPLS Pseudowire

Pseudowire is a point-to-point Layer 2 connection between two PE routers. The MPLS Pseudowire for Cable L2VPN feature supports the following pseudowire types:

- Type-4 pseudowire—This is used to transport only VLAN tagged Layer 2 Ethernet frames.
- Type-5 pseudowire—This is used to transport VLAN tagged and untagged Layer 2 Ethernet frames. This is the default pseudowire type.

Bundle254 Interface

The bundle254 (Bu254) interface is an internal bundle interface on a Cisco CMTS router that is used as a circuit identifier for all MPLS pseudowires. This internal bundle interface is created automatically on a Cisco CMTS router when you enable the MPLS pseudowire functionality using the **cable l2-vpn-service xconnect** command. Only one Bu254 interface is created to handle all the MPLS pseudowires available on the Cisco CMTS router.

The output of the **show xconnect or show cable l2-vpn xconnect command displays** the circuit identifier created by the Cisco CMTS router for all the MPLS pseudowires**.**

Ingress Process

When an upstream packet received from a cable interface of the Cisco CMTS router is identified as an L2VPN packet based on the cable modem interface and Service ID (SID), the packet goes through the ingress process. The ingress process ensures that the DOCSIS header is removed, and an MPLS label header is added to the packet according to the MPLS pseudowire configuration and the packet is sent out from the Ethernet interface of the Cisco CMTS router. The ingress process is also known as the label imposition process.

Egress Process

When a downstream packet received from an Ethernet interface of the Cisco CMTS router is identified as an L2VPN packet by the innermost MPLS label, the packet goes through the egress process. The egress process ensures that the MPLS label header is deleted from the packet and the DOCSIS header is added to the packet. Then the packet is sent out from the cable interface of the Cisco CMTS router. The egress process is also known as the label disposition process.

MPLS Pseudowire Control Plane Process

When an L2VPN-compliant CM registers with a Cisco CMTS router and conveys the L2VPN related parameters to the router, the router follows the standard Label Distribution Protocol (LDP) procedures to set up an Ethernet over MPLS pseudowire with the remote PE router. When the L2VPN-compliant CM goes offline, the Cisco CMTS router brings down the pseudowire as well. If the Cisco CMTS router has no L2VPN-compliant CM registered, then the router tears down the targeted LDP session with the remote PE router.

L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables a PE router to detect a pseudowire failure and reroute the Layer 2 service to a backup pseudowire that can continue to provide the service. The pseudowire redundancy can be implemented with either Cisco CMTS or a generic router as the PE router. When the primary pseudowire recovers from the failure, the L2VPN Pseudowire Redundancy feature provides the option to bring back the Layer 2 service to the primary pseudowire.

Each primary pseudowire can have up to three backup pseudowires, with unique priorities. For example, priority one cannot be given to two different pseudowires in the backup list. When the primary pseudowire goes down, the Cisco CMTS sends the traffic to the backup pseudowire with the highest priority. For a successful service transfer, the remote state of the backup pseudowire should already be ‘up’. Only the local state of the active pseudowire will be 'up' when the modem is BPI online. Similarly, if the backup pseudowire is in use, the local state of only that backup pseudowire will be 'up'.

If the active backup pseudowire goes down, the Cisco CMTS will use the next highest backup pseudowire whose remote state is ‘up’. However, the Cisco CMTS will not switchover from the lower priority pseudowire to the higher priority pseudowire when the backup pseudowire with the highest priority comes ‘up’. This is to prevent unnecessary switchovers between the backup pseudowires.

When the primary pseudowire recovers from the failure, the L2VPN Pseudowire Redundancy feature brings back the service to the primary pseudowire, after waiting for the time period set using the backup delay

command. The local state of the active backup pseudowire will be marked as 'down' after the primary pseudowire comes up.

MPLS Pseudowire Provisioning Methods

The MPLS Pseudowire for Cable L2VPN feature supports the following provisioning methods for pseudowires:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router. For details on the tasks required to enable MPLS, see the How to Enable MPLS on a Cisco CMTS Router.

Static Provisioning Method for MPLS Pseudowires

The static provisioning method requires the MPLS pseudowire to be statically provisioned on the CMTS using the command line interface (CLI). This type of provisioning does not require the CM configuration file to use BSOD L2VPN-compliant TLVs. For details on how to statically provision MPLS pseudowires, see the Static Provisioning of MPLS Pseudowires, on page 1014.

Dynamic Provisioning Method for MPLS Pseudowires

The dynamic provisioning method is a CM configuration file-based provisioning method and is the recommended provisioning method for creating MPLS pseudowires. For details on how to dynamically provision MPLS pseudowires, see the Dynamic Provisioning of MPLS Pseudowires, on page 1013.

The following are the benefits of dynamic provisioning of pseudowires:

- Multiple VPNs can be specified in a CM configuration file and a pseudowire can be provisioned for each VPN.
- Multiple upstream service flows and downstream classifiers can be associated with each VPN.
- Each upstream service flow can be tagged to an MPLS experimental (EXP) level for the egress WAN traffic.
- Downstream ingress WAN traffic can be classified based on the downstream MPLS-EXP range specified in each downstream classifier.
- The Cisco CMTS router will have finer control of MPLS quality of service (QoS) over cable and WAN interfaces.

For dynamic provisioning of MPLS pseudowires, you use an L2VPN-compliant CM configuration file that is stored on the Trivial File Transfer Protocol (TFTP) server. You use a common CM configuration file editor such as CableLabs Config File Editor, or a sophisticated provisioning backend system such as Broadband Access Center for Cable (BACC) to create CM configuration files.

This provisioning method requires the usage of CableLabs defined L2VPN encodings such as type, length, value (TLV) objects in the CM configuration file. These L2VPN encodings control L2VPN forwarding of upstream and downstream Ethernet frames.

You can specify the L2VPN encodings in the following ways:

- Per CM
- Per downstream classifier
- Per service flow
- Per upstream classifier

Note The CM L2VPN encoding is mandatory.

The CM L2VPN encoding contains many TLVs, out of which the two most important TLVs are VPN Identifier and NSI Encapsulation. To configure an MPLS pseudowire, you must set the NSI Encapsulation to MPLS. The other TLVs are used to specify the pseudowire identifiers in the form of source attachment individual identifier (SAII), target attachment individual identifier (TAII), and attachment group identifier (AGI).

The L2VPN encoding parameter is encoded as a general extension information (GEI) parameter in the CM configuration file. This indicates that the parameter is encoded as a subtype of the vendor-specific information type parameter using the vendor ID (0xFFFFFF).

The table lists the important CableLabs defined TLVs that are used at the top level of the CM configuration file for the MPLS Pseudowire for Cable L2VPN feature. See the BSOD specification, *Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks,* from CableLabs for *a complete list of CableLabs defined TLVs.*

Table 104: CableLabs Defined L2VPN TLVs

TLV Name	Type	Length	Value and Description
Downstream Unencrypted Traffic (DUT) Control	45.1	1	Bit 0 DUT Filtering DUT Filtering = 0: Disable (default) DUT Filtering = 1: Enable DUT Filtering
Downstream Unencrypted Traffic (DUT) CMIM	45.2	N	DUT CMIM (optional) CM Interface Mask (CMIM) limiting outgoing interfaces of DUT traffic. If the DUT CMIM is omitted, its default value includes the eCM and all implemented eSAFE interfaces, but not any CPE interfaces.
VPN Identifier	43.5.1	1 to N	An opaque octet string that identifies an L2VPN. N is vendor- specific, and the valid range is from 6 to 255.

TLV Name	Type	Length	Value and Description
NSI Encapsulation Subtype	43.5.2	n	A single NSI encapsulation format code/length/value tuple. This TLV uses any of the following values: NSI encapsulation = 0 : Other NSI encapsulation = 1 : IEEE 802.1Q (specify VLAN ID) NSI encapsulation = 2 : IEEE 802.1AD (specify Q-in-Q) NSI encapsulation = 3 : MPLS peer (specify IPv4 or IPv6 address) The value must be set to 3 to ensure MPLS pseudowire usage. The address must identify the remote PE (by its IP address assigned to the loopback interface).
Attachment Group ID	43.5.5	0 to 16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.
Source Attachment Individual ID	43.5.6	0 to 16	Opaque byte string signaled as SAII circuit for IETF Layer 2 VPN signaling protocols.
Target Attachment Individual ID	43.5.7	0 to 16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.
Ingress User Priority	43.5.8	1	Ingress IEEE 802.1 user priority value in the range of 0 to 7 encoded in the least significant three bits. Higher values indicate higher priority.

TLV Name	Type	Length	Value and Description
User Priority Range	43.5.9	2	The lower user priority value of the user priority range is encoded in the least significant three bits of the first byte, and the higher value of the range is encoded in the least significant three bits of the second byte.

Cisco-Specific L2VPN TLVs

Even though CableLabs defined L2VPN TLVs are sufficient for dynamic provisioning of MPLS pseudowires, CMTS operators can use Cisco-specific TLVs at the top level of the CM configuration file to enable additional functions.

This table lists the new Cisco-specific TLVs that are defined for the MPLS Pseudowire for Cable L2VPN feature.

Table 105: Cisco-Specific L2VPN TLVs

TLV Name	Type	Length	Value	Description
MPLS-PW-TYPE	43.5.43.36	1	• 4 = Type-4 Ethernet VLAN • 5 = Type-5 Ethernet port	The Cisco CMTS router interprets this subtype as MPLS pseudowire type (Type-4 or Type-5). If this TLV value is not specified, then the router accepts the default value (5) for Type-5.

TLV Name	Type	Length	Value	Description
MPLS-VCID	43.5.43.38	4	4 bytes unsigned number = MPLS VCID	This subtype is interpreted as MPLS VCID. This TLV is ignored, and the value of TAII is used as VCID for the pseudowire, if the following conditions are met: • The CableLabs BSOD specification-compliant TLVs, SAII and TAII, are present in the CM configuration file. • Both are of 4 bytes length. • Value of SAII is equal to TAII.
MPLS-PEERNAME	43.5.43.39	N	ASCII encoded data	The Cisco CMTS router interprets this optional subtype as MPLS peer name in ASCII encoded data.

This table lists the new Cisco-specific type, length, values (TLVs) that are defined for the L2VPN Pseudowire Redundancy feature.

Table 106: Cisco-Specific L2VPN TLVs for Pseudowire Redundancy

TLV Name	Type	Length	Value	Description
BACKUP-PW	45.5.43.40	N	Backup pseudowire related parameters	The Cisco CMTS router interprets this subtype as related parameters for the MPLS backup pseudowire. This TLV indicates the start of a new backup pseudowire.

TLV Name	Type	Length	Value	Description
BACKUP-PEERIP	43.5.43.40.1	4	IP address of the backup peer (IPv4)	The Cisco CMTS router interprets this optional subtype as the peer IP address of the MPLS backup pseudowire. This TLV is an IPv4 address.
BACKUP-PEERNAME	43.5.43.40.2	N	ASCII encoded data	The Cisco CMTS router interprets this optional subtype as the MPLS backup peer name in ASCII encoded data. This TLV is resolved to IPv4 address through DNS.
BACKUP-MPLS-VCID	43.5.43.40.3	4	4 bytes unsigned number = MPLS VCID for backup pseudowire	The Cisco CMTS router interprets this subtype as the VCID of the backup pseudowire. This TLV is ignored, and the value of TAII is used as the VCID for the pseudowire, if the following conditions are met: • The CableLabs BSOD specification-compliant TLVs, SAII, and TAII, are present in the CM configuration file. • SAII, and TAII are of 4 bytes length. • Value of SAII is equal to TAII.

TLV Name	Type	Length	Value	Description
BACKUP-MPLS-PRIORITY	43.5.43.40.4	1	1 byte unsigned number = priority for the backup pseudowire	The Cisco CMTS router interprets this subtype as the MPLS priority. Each primary pseudowire can have up to three backup pseudowires, with unique priorities. The priority indicates the order in which the CMTS should switch to the backup peer when the primary peer is down.
BACKUP-ENABLE-DELAY	43.5.43.41	1	1 byte unsigned number = number of seconds	The Cisco CMTS router interprets this subtype as the number of seconds the backup pseudowire should wait to take over after the primary pseudowire goes down. If the TLV value is not specified, then the router uses the default value of 0 seconds.
BACKUP-DISABLE-DELAY	43.5.43.42	1	1 byte unsigned number = number of seconds	The Cisco CMTS router interprets this subtype as the number of seconds the primary pseudowire should wait to take over after the remote state of the primary pseudowire comes up. If the TLV value is not specified, then the router uses the default value of 0 seconds.

TLV Name	Type	Length	Value	Description
BACKUP-DISABLE-NEVER	43.5.43.43	1	1 byte unsigned number = never disable backup pseudowire	The Cisco CMTS router interprets this subtype as a flag indicating that the backup pseudowire should not be disabled even after the primary pseudowire comes up. If this TLV is not present, the router takes the default action of reverting back to the primary pseudowire.

How to Enable MPLS on a Cisco CMTS Router

Perform the following tasks in the same order to enable MPLS on a Cisco CMTS router:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router.

Configuring an LDP Router ID

The **mpls ldp router-id** command allows you to assign an interface IP address as the LDP router ID.

The normal process to determine the LDP router ID is as follows:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address is not considered as the router ID of the local LDP ID under the following circumstances:

1. If the loopback interface has been explicitly shut down.
2. If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.
3. If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, ensure that the routing protocol in use is configured to advertise the corresponding /32 network. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router. The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the **mpls ldp router-id**

command is delayed until it is necessary to select an LDP router ID, which is the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

Before You Begin

Ensure that the specified interface is operational before assigning it as the LDP router ID.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Router(config)# mpls ip`	Enables the dynamic MPLS forwarding function on the specified Gigabit Ethernet interface.
Step 4	**mpls ldp router-id loopback** interface-number [**force**] **Example:** `Router(config)# mpls ldp router-id loopback 2030 force`	Specifies the IP address of the loopback interface as the LDP router ID.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring MPLS on a Gigabit Ethernet Interface

MPLS forwarding and Label Distribution Protocol must be enabled on 1-port or 10-port GE interfaces of the Cisco CMTS router to ensure that the router establishes MPLS label-switched path (LSP) to the remote PE routers. This section explains how to enable MPLS forwarding and LDP on a Gigabit Ethernet interface.

Note Configuration steps are similar for 1-port and 10-port GE interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** slot/subslot/port **Example:** `Router(config)# interface gigabitethernet 3/0/0`	Enters interface cable configuration mode and specifies the Gigabit Ethernet interface.
Step 4	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables the dynamic MPLS forwarding function on the specified Gigabit Ethernet interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface cable configuration mode and enters privileged EXEC mode.

Configuring an MPLS Label Distribution Protocol

The MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP VPNs that support multiple levels of services. This section explains how to configure an MPLS label distribution protocol on a Gigabit Ethernet interface.

Note Ensure that the loopback interface with the IP address is present on each PE router using the **show ip interface brief** command before configuring an MPLS label distribution protocol. This loopback interface identifies the Cisco CMTS router as the peer IP address of the pseudowire.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** slot/subslot/port **Example:** `Router(config)# interface gigabitethernet 3/0/0`	Enters interface cable configuration mode and specifies the Gigabit Ethernet interface.
Step 4	**mpls label protocol ldp** **Example:** `Router(config-if)# mpls label protocol ldp`	Enables MPLS LDP parameters on the specified Gigabit Ethernet interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface cable configuration mode and enters privileged EXEC mode.

Enabling the Cisco CMTS Support for MPLS Pseudowire for Cable L2VPN

You must enable the MPLS tunnel traffic on the network side of the interface to support configuration of MPLS pseudowires on a Cisco CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2-vpn-service xconnect nsi mpls** **Example:** `Router(config)# cable l2-vpn-service xconnect nsi mpls`	Enables the MPLS tunnel traffic, where:
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

How to Provision MPLS Pseudowires

You can provision MPLS pseudowires in the following ways:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router.

Dynamic Provisioning of MPLS Pseudowires

The dynamic provisioning method supports the following types of configurations:

- BSOD Specification-Based MPLS Pseudowire Provisioning

- Type-4 MPLS Pseudowire Provisioning Using the CM Configuration File
- Type-5 MPLS Pseudowire Provisioning Using the CM Configuration File

See the Configuration Examples for Dynamic Provisioning of MPLS Pseudowires for details about the dynamic provisioning method using the CM configuration file.

Note We recommend that you use the dynamic provisioning method instead of the static provisioning method for MPLS pseudowires.

Static Provisioning of MPLS Pseudowires

Static provisioning of MPLS pseudowires is not required if you have already provisioned MPLS pseudowires using the dynamic provisioning method.

Note
- You can provision only one MPLS pseudowire per L2VPN.
- Only one Ethernet service instance can exist per MPLS pseudowire configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2vpn** *mac-address [customer-name]* **Example:** `Router(config)# cable l2vpn 0000.396e.6a68 customer1`	Specifies L2VPN MAC address and enters L2VPN *configuration mode.*
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 2000 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode.

	Command or Action	Purpose
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*] **Example:** `Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire.
Step 6	**cable set mpls-experimental** *value* **Example:** `Router(config-ethsrv)# cable set mpls-experimental 7`	Specifies the experimental bit on the MPLS pseudowire. The valid range is from 0 to 7.
Step 7	**end** **Example:** `Router(config-ethsrv)# end`	Exits Ethernet service configuration mode and enters global configuration mode.

How to Configure L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables you to switch to backup pseudowires when the primary pseudowire fails. The feature also allows the Cisco CMTS to resume operation on the primary pseudowire after it comes back up.

Configuring the Backup Pseudowire

You can configure up to three backup pseudowires for a primary pseudowire. The priority of each backup pseudowire has to be unique.

A backup pseudowire is uniquely identified by a combination of IP address or hostname and VCID. Only the IP address or hostname and VCID can be configured for the backup peer, the remaining parameters are the same as the primary pseudowire.

Backup pseudowires can also be configured using the DOCSIS configuration files. Cisco Specific L2VPN TLVs lists Cisco-specific TLVs introduced in Cisco IOS Release 12.2(33)SCF to support the L2VPN Pseudowire Redundancy feature.

Perform the steps given below to configure a backup pseudowire.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2vpn** *mac-address* **Example:** `Router(config)# cable l2vpn 0011.0011.0011`	Specifies L2VPN MAC address and enters L2VPN *configuration mode.*
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 1 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode.
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire and enters xconnect configuration mode.
Step 6	**backup peer** *peer-ip-address vc-id* [priority value] **Example:** `Router(config-xconn)# backup peer 10.3.3.3 33 priority 2`	Specifies the backup pseudowire and its priority. The priority keyword is optional, if only one backup pseudowire is configured. When multiple backup pseudowires are configured, it is required.
Step 7	**end** **Example:** `Router(config-xconn)# end`	Exits xconnect configuration mode and enters Privileged EXEC mode.

Configuring Backup Delay

Perform the steps given below to configure the period the backup pseudowire should wait to take over after the primary pseudowire goes down. You can also specify how long the primary pseudowire should wait after it becomes active to take over from the backup pseudowire.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2vpn** *mac-address* **Example:** `Router(config)# cable l2vpn 0011.0011.0011`	Specifies the L2VPN MAC address and enters L2VPN *configuration mode.* • *mac-address*—MAC address of a CM.
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 1 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode. • *id*—Service instance ID. • service-type—Service type for the instance.
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire and enters xconnect configuration mode. • *peer-ip-address*—IP address of the remote PE router. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—32-bit identifier of the virtual circuit between the PE routers. • **encapsulation mpls**—Specifies MPLS as the tunneling method.
Step 6	Do one of the following: • **backup delay** enable-delay-period {disable-delay-period | never} •	Specifies the period to wait before enabling or disabling the backup pseudowire. • *enable-delay-period*—Number of seconds the backup pseudowire should wait to take over after the primary pseudowire goes down. The valid range is from 0 to 180 seconds, with a default value of 0.

	Command or Action	Purpose
	Example: `Router(config-xconn)# backup delay 10 10` **Example:** `Router(config-xconn)# backup delay 10 never`	• *disable-delay-period*—Number of seconds the primary pseudowire should wait after it becomes active to take over from the backup pseudowire. The valid range is from 0 to 180 seconds, with a default value of 0. • **never**—Specifies the primary pseudowire should not be reactivated after moving to the backup pseudowire.
Step 7	**end** **Example:** `Router(config-xconn)# end`	Exits xconnect configuration mode and enters privileged EXEC mode.

Performing Manual Switchover

Perform the steps given below to perform a manual switchover to the primary or backup pseudowire. The **cable l2vpn xconnect backup force-switchover** command can also be used to forcefully switch to the backup pseudowire for planned outages of the primary remote peer.

Note A manual switchover can be made only to an available member in the redundancy group. If the pseudowire specified in the command is not available, the command will be rejected.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cable l2vpn xconnect backup force-switchover peer 10.10.1.1 123** **Example:** `Router# cable l2vpn xconnect backup force-switchover peer 10.10.1.1 123`	Specifies that the router should switch to the backup or to the primary pseudowire.

Troubleshooting Tips

The following commands help you troubleshoot an improper MPLS pseudowire configuration:

- **show ip interface brief—**Helps verify that the loopback interface with the IP address is present on each PE router.
- **show mpls l2transport vc—**Helps verify information about primary and backup pseudowires that have been enabled to route Layer 2 packets on a router.
- **show xconnect all—**Helps verify information about all xconnect attachment circuits and primary and backup pseudowires.
- **show cable l2-vpn xconnect mpls-vc-map—**Helps verify that the primary and backup pseudowires are configured properly.

Configuration Examples for MPLS Pseudowire for Cable L2VPN

The following sections provide MPLS pseudowire configuration examples for the static and dynamic provisioning methods:

Configuration Example for Static Provisioning of MPLS Pseudowires

The following example shows CLI-based provisioning of an MPLS pseudowire:

```
Router> enable
Router# configure terminal
Router(config)# cable l2vpn 0000.396e.6a68 customer2
Router(config-l2vpn)# service instance 2000 ethernet
Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
Router(config-ethsrv)# cable set mpls-experimental 7
```

Configuration Examples for Dynamic Provisioning of MPLS Pseudowires

The following sections provide MPLS pseudowire provisioning examples based on BSOD CableLabs specification, Type-4, and Type-5 TLVs using the CM configuration file:

BSOD Specification-Based MPLS Pseudowire Provisioning: Example

The following example shows an MPLS pseudowire configuration based on BSOD CableLabs specification:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN sub-type)
 =
        T01 (VPN Id) = 02 34 56 00 02 # VPNID=0234650002
        T02 (NSI) = 04 05 01 0a 4c 01 01# [04=mpls] [05=len][01=ipv4][IP=10.76.1.1]
        T05 (AGI) = 01 01 07 d1 # AGI = 0x010107d1
        T06 (SAII) = 00 00 07 d1 # SAII = TAII = VCID = 0x7d1 = 2001
```

```
        T07 (TAII) = 00 00 07 d1
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)  =
            S01 (VPNID) =   02 34 56 00 02
            S08 (UserPrio) = 01

24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) =   02 34 56 00 02
            S08 (UserPrio) = 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 06
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 00 20 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 21 40 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)  = 41 ff ff
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 02
   S43 (Vendor Specific Options)
```

```
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)

              S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 03 04
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
              S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 05 06
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
              S01 (VPNID) = 02 34 56 00 02
```

Type-4 MPLS Pseudowire Provisioning Using the CM Configuration File: Example

The following example shows a CM configuration file-based provisioning of a Type-4 MPLS pseudowire:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 = 2001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 03 # VPN-ID = "0234560003"
T043 (Cisco Vendor Specific) =  2b 16
S008 (Vendor ID) = 00 00 0c Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0b b9 # = 3001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 04 # VPN-ID = "0234560004"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0f a1 # = 4001 VCID
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
```

```
S034 (MPLS-EXP-SET) = 22 05 # MPLSEXP-INGRESS= 5
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 03
       T043 (Cisco Vendor Specific) =  2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 06

# MPLSEXP-INGRESS= 6
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 04

# MPLSEXP-INGRESS= 4
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S05 (Rule Priority) = 2
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S05 (Rule Priority) = 3
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S05 (Rule Priority) = 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S035 (MPLS-EXP_RANGE) = 23 02  03 # MPLSEXP-EGRESS_RANGE= 2 - 3
   S05 (Rule Priority) = 2
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
```

```
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) =  02 34 56 00 03
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 04  05 # MPLSEXP-EGRESS_RANGE= 4 - 5
   S05 (Rule Priority = 3
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 00  01 # MPLSEXP-EGRESS_RANGE= 0 - 1
   S05 (Rule Priority) = 4
```

Type-5 MPLS Pseudowire Provisioning Using the CM Configuration File: Example

The following example shows a CM configuration file-based provisioning of a Type-5 MPLS pseudowire:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 05 # MPLSPWTYPE= Type5 - Ethernet-Port Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 # = 2001 VCID
45 (L2VPN CMIM) = 02 04 ff ff ff ff 01 01 01
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S034 (MPLS-EXP-SET) = 22 04 # MPLS-EXP-SET at INGRESS= 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
```

Configuration Examples for L2VPN Pseudowire Redundancy

The following sections provide L2VPN pseudowire redundancy configuration examples using the CM configuration file:

Example: Configuring Backup Pseudowire Peer and VC ID

The following example shows how to provision a file-based backup peer router based on the CM configuration:

PE Router 1

```
cable l2vpn 0025.2e2d.7252
 service instance 1 ethernet
  encapsulation default
  xconnect 10.76.2.1 400 encapsulation mpls
   backup peer 10.76.2.1 600 priority 4
```

PE Router2

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup peer 10.3.3.3 33 priority 2
   backup delay 10 10
```

Example: Configuring Backup Delay

The following example shows how to configure a backup delay to determine how much time should elapse before a secondary line status change after a primary line status has been changed.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup delay 10 10
```

Example: L2VPN Backup MPLS Pseudowire Provisioning Using the CM Configuration File

The following example shows how to provision an L2VPN Backup MPLS pseudowire based on the CM configuration file:

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 3
43 (Vendor Specific Options)
   S08 (Vendor ID)      = ff ff ff
   S005 (Unknown sub-type)      = 01 04 32 30 32 30 02 07 04 05 01 0a 4c 02 01 2b 15 26 04
 00 00 00 14 28 10 01 05 01 0a 4c 02 01 03 04 00 00 07 08 04 01 05 28 0d 01 05 01 0a 4c 02
 03 03 04 00 00 00 15 28 10 01 05 01 0a 4c 02 01 03 04 00 00 b1 8e 04 01 01 29 01 03 2a 01
 01
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 4
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 2000000
   S09 (Max Traffic Burst)              = 3200
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options)
       T08 (Vendor ID)      = ff ff ff
       T005 (Unknown sub-type)      = 01 04 32 30 32 30
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 3000000
   S09 (Max Traffic Burst)              = 250000
29 (Privacy Enable)             = 1
```

Verifying the MPLS Pseudowire Configuration

Use the following **show** commands to verify the MPLS pseudowire configuration:

- **show mpls ldp discovery**
- **show cable l2-vpn xconnect**
- **show xconnect**
- **show mpls l2transport vc**

To verify the LDP router ID and the status of the LDP discovery process, use the **show mpls ldp discovery command** as **shown in the following example:**

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    10.10.1.1:0
    Discovery Sources:
    Targeted Hellos:
        10.10.1.1 -> 10.76.1.1 (ldp): active/passive, xmit/recv
            LDP Id: 10.76.1.1:0
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems, use the **show cable l2-vpn xconnect** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address  VCID       CktID      Cable Intf  SID  Customer
Name/VPNID
0000.396e.6a68  101.1.0.2       221        Bu254:221    Cable7/0/0  1    customer1
0014.f8c1.fd66  10.76.1.1       2004       Bu254:5121   Cable7/0/0  8
0019.474a.d566  10.76.1.1       2001       Bu254:5122   Cable7/0/0  4    0234560002
0019.474a.d42e  10.76.1.1       2002       Bu254:2003   Cable7/0/0  5    0234560003
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems (when pseudowire redundancy is not configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show cable l2-vpn xconnect mpls-vc-map** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID   Type  Prio   CktID      Cable Intf SID  Customer
                                                                            Name/VPNID
0025.2e2d.7252  10.76.2.1      400    Prim*      Bu254:400    Cable8/0/3  1
0014.f8c1.fd46  10.2.3.4       1000   Prim*      Bu254:1000   Cable8/0/0  1   2020
0014.f8c1.fd46  10.76.2.1      1800   Prim*      Bu254:1800   Cable8/0/0  1   2021
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show cable l2-vpn xconnect mpls-vc-map** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID   Type  Prio   CktID      Cable Intf SID  Customer
                                                                            Name/VPNID
0025.2e2d.7252  10.76.2.1      400    Prim*      Bu254:400    Cable8/0/3  1
                10.76.2.1      600    Bkup    4  Bu254:600
0014.f8c1.fd46  10.2.3.4       1000   Prim*      Bu254:1000   Cable8/0/0  1   2020
                10.76.2.1      45454  Bkup    1  Bu254:45454
0014.f8c1.fd46  10.76.2.1      1800   Prim*      Bu254:1800   Cable8/0/0  1   2021
                10.2.3.4       55     Bkup    1  Bu254:55
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire, use the show cable l2-vpn xconnect command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map state
Peer IP Address  VCID       STATE MAC Address    Customer Name/VPNID  STATE
101.1.0.2        22         DOWN  0000.396e.6a68  customer1            UP
10.76.1.1        2004       UP    0014.f8c1.fd66                       UP
```

```
10.76.1.1        2001       UP    0019.474a.d566  0234560002           UP
10.76.1.1        2002       UP    0019.474a.d42e  0234560003           UP
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire (when pseudowire redundancy is not configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show cable l2-vpn xconnect mpls-vc-map state** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address    Peer IP Address  VCID   Type  Prio  State  Customer Name/VPNID  State
0025.2e2d.7252  10.76.2.1       400    Prim*        UP                         UP
0014.f8c1.fd46  10.2.3.4        1000   Prim*        UP    2020                 UP
0014.f8c1.fd46  10.76.2.1       1800   Prim*        UP    2021                 UP
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show cable l2-vpn xconnect mpls-vc-map state** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address    Peer IP Address  VCID   Type  Prio  State  Customer Name/VPNID  State
0025.2e2d.7252  10.76.2.1       400    Prim*        UP                         UP
                10.76.2.1       600    Bkup    4    UP                         STDBY
0014.f8c1.fd46  10.2.3.4        1000   Prim*        UP    2020                 UP
                10.76.2.1       45454  Bkup    1    UP    2020                 STDBY
0014.f8c1.fd46  10.76.2.1       1800   Prim*        UP    2021                 UP
                10.2.3.4        55     Bkup    1   DOWN   2021                 STDBY
```

To verify information about the MPLS pseudowire mapping for a particular MAC address of a CM (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show cable l2-vpn xconnect mpls-vc-map** command as **shown in the following example:**

```
Router# show cable l2-vpn xconnect mpls-vc-map
0025.2e2d.7252
MAC Address    Peer IP Address  VCID Type  Prio   CktID    Cable Intf SID Customer
                                                                        Name/VPNID
0025.2e2d.7252  10.76.2.1       400  Prim*      Bu254:400  Cable8/0/3  1
                10.76.2.1       600  Bkup    4  Bu254:600
```

To verify the detailed information about the MPLS pseudowire mapping for a CM (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), use the **show mpls l2-vpn xconnect mpls-vc-map verbose** command as **shown in the following examples.**

The following example shows the information for a modem for which pseudowires were configured using backup peer command:

```
Router# show cable l2-vpn xconnect mpls-vc-map
0025.2e2d.7252 verbose
MAC Address                    : 0025.2e2d.7252
Customer Name                  :
Prim Sid                       : 1
Cable Interface                : Cable8/0/3
MPLS-EXP                       : 0
PW TYPE                        : Ethernet
Backup enable delay            : 0 seconds
Backup disable delay           : 0 seconds
Primary peer
Peer IP Address (Active)       : 10.76.2.1
XConnect VCID                  : 400
Circuit  ID                    : Bu254:400
Local State                    : UP
Remote State                   : UP
Backup peers
Peer IP Address                : 10.76.2.1
XConnect VCID                  : 600
Circuit  ID                    : Bu254:600
```

```
Local State                          : STDBY
Remote State                         : UP
Priority                             : 4
Total US pkts                        : 0
Total US bytes                       : 0
Total US pkts   discards             : 0
Total US bytes  discards             : 0
Total DS pkts                        : 0
Total DS bytes                       : 0
Total DS pkts   discards             : 0
Total DS bytes  discards             : 0
```

The following example shows the information for a modem for which pseudowires **were created using the modem configuration file:**

```
Router# show cable l2-vpn xconnect mpls-vc-map
0014.f8c1.fd46 verbose
MAC Address                          : 0014.f8c1.fd46
Prim Sid                             : 3
Cable Interface                      : Cable8/0/0
L2VPNs provisioned                   : 1
DUT Control/CMIM                     : Disable/0x8000FFFF
VPN ID                               : 2020
L2VPN SAID                           : 12289
Upstream SFID Summary                : 15
Downstream CFRID[SFID] Summary       : Primary SF
CMIM                                 : 0x60
PW TYPE                              : Ethernet
MPLS-EXP                             : 0
Backup enable delay                  : 3 seconds
Backup disable delay                 : 1 seconds
Primary peer
Peer IP Address (Active)             : 10.2.3.4
XConnect VCID                        : 1000
Circuit  ID                          : Bu254:1000
Local State                          : UP
Remote State                         : UP

Backup peers
Peer IP Address                      : 10.2.3.4
XConnect VCID                        : 21
Circuit  ID                          : Bu254:21
Local State                          : STDBY
Remote State                         : DOWN
Priority                             : 2
Peer IP Address                      : 10.76.2.1
XConnect VCID                        : 1800
Circuit  ID                          : Bu254:1800
Local State                          : STDBY
Remote State                         : DOWN
Priority                             : 5
Peer IP Address                      : 10.76.2.1
XConnect VCID                        : 45454
Circuit  ID                          : Bu254:45454
Local State                          : STDBY
Remote State                         : DOWN
```

To verify information about all attachment circuits and pseudowires, use the **show xconnect** command as **shown in the following example:**

```
Router# show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)           UP mpls 10.76.1.1:2001                UP
UP     ac   Bu254:2002(DOCSIS)           UP mpls 10.76.1.1:2002                UP
```

```
UP      ac    Bu254:2004(DOCSIS)           UP mpls 10.76.1.1:2004               UP
DN      ac    Bu254:22(DOCSIS)             UP mpls 101.1.0.2:22                 DN
```

To verify information about MPLS virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a Cisco CMTS router, use the **show mpls l2transport vc** command as **shown in the following example:**

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Bu254          DOCSIS 2002                10.76.1.1       2002       UP
Bu254          DOCSIS 2003                10.76.1.1       2003       UP
Bu254          DOCSIS 2004                10.76.1.1       2004       DOWN
Bu254          DOCSIS 2017                10.76.1.1       2017       UP
Bu254          DOCSIS 2018                10.76.1.1       2018       UP
Bu254          DOCSIS 2019                10.76.1.1       2019       UP
```

Additional References

The following sections provide references related to the MPLS pseudowire functionality.

Related Documents

Related Topic	Document Title
Cisco IOS CMTS Cable Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
L2VPN Support Over Cable	*Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_l2vpn.html
Any Transport over MPLS	*Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4T* http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1mt/mp-any-transport.html
Label Distribution Protocol	MPLS Label Distribution Protocol http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ftldp41.html

Standards

Standard	Title
CM-SP-L2VPN-I08-080522	*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks*

Standard	Title
L2VPN-N-10.0918-2	*L2VPN MPLS Update*

MIBs

MIB	MIBs Link
• DOCS-L2VPN-MIB • CISCO-IETF-PW-MIB • CISCO-CABLE-L2VPN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 3985	*Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*
RFC 4385	*Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*
RFC 4446	*IANA Allocations for Pseudowire Edge-to-Edge Emulation (PWE3)*
RFC 4447	*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*
RFC 4448	*Encapsulation Methods for Transport of Ethernet over MPLS Networks*
RFC 5085	*Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

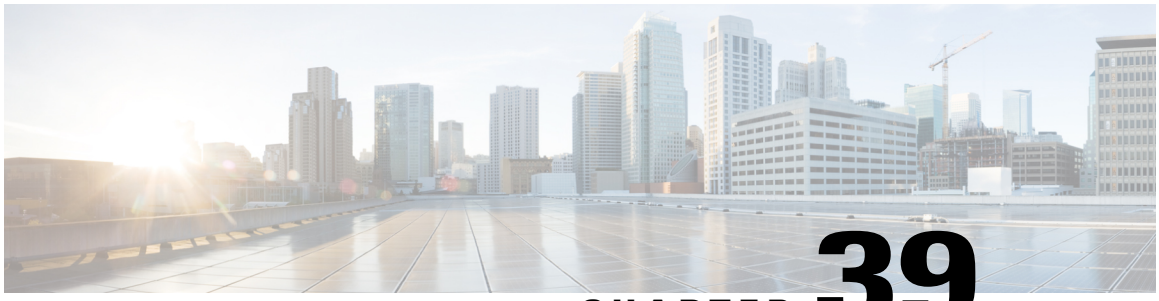
Feature Information for MPLS Pseudowire for Cable L2VPN

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 107: Feature Information for MPLS Pseudowire for Cable L2VPN

Feature Name	Releases	Feature Information
MPLS Pseudowire for Cable L2VPN	12.2(33)SCC	The MPLS Pseudowire for Cable L2VPN feature is an extension to the existing DOCSIS L2VPN functionality using an Ethernet VLAN on Cisco uBR10012 routers and Cisco uBR7200 Series routers. The following commands were introduced or modified: • **cable l2vpn** • **cable l2-vpn-service xconnect** • **cable set mpls-experimental** • **service instance** • **show cable l2-vpn xconnect** • **show mpls l2transport vc** • **show xconnect** • **xconnect**
L2VPN Pseudowire Redundancy	12.2(33)SCF	The L2VPN Pseudowire Redundancy feature enables you to configure a backup pseudowire in case the primary pseudowire fails. The following sections provide information about this feature: The following commands were introduced or modified: • **backup delay** • **backup peer** • **cable l2-vpn xconnect backup force-switchover** • **show cable l2vpn xconnect** • **show mpls l2transport vc** • **show xconnect**



CHAPTER 39

Point-to-PointProtocoloverEthernetTermination on the Cisco CMTS

First Published: February 14, 2008

Last Updated: December 18, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco uBR7246VXR and Cisco uBR7225VXR CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS BC releases.

This chapter describes the PPPoE Termination feature, which allows service providers to extend their existing PPP dial-up provisioning systems to users on cable networks by encapsulating the PPP packets within Ethernet MAC frames.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for PPPoE Termination

The PPPoE Termination feature has the following prerequisites:

- The PPPoE Termination feature is supported only on the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
- The Cisco CMTS router must be running Cisco IOS Release 12.2(4)BC1a or later release. In addition, to support the PPPoE Termination feature, the software image name must include the IP+ feature set (the letters "i" and "s" must appear in the software image name).
- To support PPPoE Termination on bundled cable interfaces, the Cisco CMTS router must be running Cisco IOS Release 12.2(8)BC2 or later release.
- Client software must support the PPPoE Termination protocol. If the computer operating system does not include such support, the user can use client software such as WinPoet.
- If planning on a large number of PPPoE sessions and traffic, increase the size of the packet hold queues on the WAN interfaces (ATM, DPT, Gigabit Ethernet, etc.), using the **hold-queue** *packet-size* {**in** | **out**} command. For example:

```
Router(config)# interface gigabitethernet 1/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
Router(config-if)#
```

Restrictions for PPPoE Termination

The PPPoE Termination feature has the following restrictions and limitations:

- The PPPoE Termination feature is only supported on the Cisco uBR7100 series routers and Cisco uBR7246VXR router, using Cisco IOS Release 12.2(4)BC1a or later. It is not supported on the Cisco uBR10012 router.
- The PPPoE Termination feature is not supported on any Cisco CMTS router when using Cisco IOS Release 12.1 EC.
- Effective with Cisco IOS Release 12.2(33)SCD, the PPPoE Termination feature is not supported on the Cisco uBR7200 router.
- PPPoE Forwarding is not supported on any Cisco CMTS.

- Table 108: Absolute Maximum Number of PPPoE Sessions, on page 1035 shows the absolute maximum number of PPPoE sessions supported on the Cisco uBR7100 series routers, and on the Cisco uBR7246VXR router when using different processor cards.

Table 108: Absolute Maximum Number of PPPoE Sessions

Processor	Absolute Maximum Number of PPPoE Sessions
Cisco uBR7100 series	4000
NPE-225	4000
NPE-300[64]	4000
NPE-400	8000
NPE-G1	10000

64 The NPE-300 processor reached its end-of-life milestone on August 15, 2001.

Note The maximum number of active, simultaneous PPPoE sessions is much less (approximately 600 to 800), depending on the number of amount of memory onboard the processor card, the type of cable interface cards being used, the bandwidth being consumed by each user, and the router's configuration.

Information About PPPoE Termination

This section describes the PPPoE Termination feature:

Feature Overview

The Point-to-Point Protocol over Ethernet (PPPoE) feature supports PPPoE on cable interfaces, allowing service providers to extend their existing PPP dial-up provisioning systems to users on cable networks. When PPPoE Termination is enabled, the Cisco CMTS encapsulates PPP packets in Ethernet frames within PPPoE sessions.

When the Cisco CMTS receives PPPoE traffic from PPPoE sessions that are initiated by the user's PC, the Cisco CMTS either terminates the PPPoE sessions on the cable interface or transmits the PPPoE traffic through a secure tunnel connection, depending on the Cisco CMTS configuration. The following are the most typical configurations:

- Internet access—For residential customers and other users who want only basic Internet access, traffic is sent out on the WAN interface as standard IP packets. The service provider can use the same provisioning systems as they use for their dial-up users and other broadband users. The PPPoE session exists only between the cable modem and Cisco CMTS, simplifying network management and configuration.

- Secure corporate access—For businesses or telecommuters, traffic is forwarded over a Layer 2 point-to-point Tunneling Protocol (L2TP) tunnel to a L2TP network server (LNS) to create secure corporate intranet access. Cable modem users can access company resources as if they were directly connected to the corporate network, without compromising network security. This tunnel can be built over whatever interface is being used with the corporate site (Ethernet, ATM, and so forth).

When using the L2TP tunnel configuration, the Cisco CMTS acts as the L2TP Access Concentrator (LAC), or Network Access Server (NAS). The endpoint of the tunnel is the LNS, which can be a router such as a Cisco 6400 Carrier-Class Broadband Aggregator.

When the cable modem, acting as a bridge, receives its PPPoE session traffic, it forwards the traffic on to the hosts and other customer premises equipment (CPE) devices that are connected behind it. Users at these hosts or CPE devices can use standard PPP to log on to the cable network and obtain their IP addresses and other network information. Users can automate this procedure by using a router that supports PPPoE or by using standard PPPoE software, such as WinPoet.

User names and passwords can be included in the Cisco CMTS configuration, or the service provider can use the same Remote Authentication Dial-In User Service (RADIUS) authentication servers as they use for their dial-up and digital subscriber line (DSL) users. For example, the Cisco Subscriber Registration Center (CSRC) provides an Access Registrar that provides RADIUS server authentication.

The PPPoE Termination feature supports simultaneous use of PPPoE clients and Dynamic Host Configuration Protocol (DHCP) clients behind the same cable modems. Subscribers can use PPPoE for their initial log on to the cable network, and then use DHCP to allow their other PCs and other hosts to obtain IP addresses for network access.

Note The Cisco CMTS routers do not support PPPoE Forwarding, which receives PPPoE packets from an incoming interface and forwards them out on an outgoing interface. The Cisco uBR7100 series routers do automatically forward PPPoE traffic when configured for MxU bridging mode (which is supported only on Cisco IOS Release 12.1 EC), but this is a consequence of the bridging configuration and not due to any PPPoE support.

Benefits

The PPPoE Termination feature provides the following benefits to cable service providers and their partners and customers:

- PPPoE complements and does not interfere with the standard DOCSIS registration and authentication procedures that are used for cable modems.
- PPPoE can be used on existing customer premise equipment, by extending the PPP session over the bridged Ethernet LAN to the PC (host).
- PPPoE preserves the point-to-point session used by ISPs in a dial-up model, without requiring an intermediate set of IP communications protocols.
- Service providers can use their existing dial-up PPP provisioning and authentication systems for users on the cable network.
- PPPoE supports the security features, such as Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), that are built into PPP systems.
- Service providers can support both PPPoE clients and DHCP-based hosts behind the same cable modem.

How to Configure the PPPoE Termination Feature

Note For Point-to-Point over Ethernet (PPPoE) configuration on the Cisco uBR7200 series routers beginning in Cisco IOS Release 12.2(33)SCA, the **bba-group** command replaces the **vpdn-group** command. The software will automatically convert an existing **vpdn-group** configuration to **bba-group** global configuration. After the configuration of **bba-group**, you cannot configure PPPoE at the VPDN level. You need to use the **bba-group** configuration.

This section describes the following tasks that are needed to implement the PPPoE Termination feature. All procedures are required, depending on the router's configuration.

Enabling VPDN Operations on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to enable virtual private dialup network (VPDN) operations on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). This procedure must be done before performing any of the other configuration procedures.

Note This procedure also must be performed on the Cisco router that is acting as the L2TP network server (LNS).

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**buffers small** {**initial** | **max-free** | **permanent**} **1024** **Example:** `Router(config)# buffers small initial 1024` **Example:** `Router(config)# buffers small max-free 1024` **Example:** `Router(config)# buffers small permanent 1024` **Example:** `Router(config)#`	(Optional) Increases the size of the buffers on the router that are used for small packets to account for the larger number of keepalive packets that are sent during PPPoE sessions. **Note** Repeat this command for each type of small packet buffers.
Step 4	**vpdn enable** **Example:** `Router(config)# vpdn enable` **Example:** `Router(config)#`	Enables virtual private dial-up networking (VPDN).
Step 5	**vpdn logging** **Example:** `Router(config)# vpdn logging` **Example:** `Router(config)#`	(Optional) Enable logging for VPDN operations. Logging is automatically disabled by default (**no vpdn logging**) when you enable VPDN. Use this command to enable logging.
Step 6	**username** *user-name* **password** [*level*] *password* **Example:** `Router(config)# username pppoe-user1@client.com password 0 pppoepassword` **Example:** `Router(config)#`	Specifies a username and password for each user to be granted PPPoE access: • *user-name* = Username that the user uses to log in. • *level* = (Optional) Encryption level for the password. The valid values are 0 (default, the following password is not encrypted) and 7 (the following password is encrypted—this option is typically used only when cutting and pasting configurations from other routers). • *password* = Password that the above user must use to log in and create a PPPoE user session.

	Command or Action	Purpose
		Note This step is not required if you are using an external server, such as a RADIUS server, to perform user authentication.
Step 7	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Configuring a Virtual Template on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual template on the Cisco CMTS router when it is acting as a LAC. This procedure is required because the Cisco CMTS uses the virtual template to configure the virtual interfaces it creates for each individual PPPoE session.

Note At least one virtual template must be created on the router to support PPPoE sessions from cable modem users.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1` **Example:** `Router(config-if)#`	Select the number of the virtual-template interface to be configured and enters interface configuration mode. **Note** You can create up to 200 virtual interfaces on each router.
Step 4	**ip unnumbered** *interface* **Example:** `Router(config-if)# ip unnumbered Ethernet2/0` **Example:** `Router(config-if)#`	Enables the virtual template interfaces to process IP packets by using the IP address of the specified interface, as opposed to assigning a unique IP address to each virtual interface.
Step 5	**ip mtu 1492** **Example:** `Router(config-if)# ip mtu 1492` **Example:** `Router(config-if)#`	Configures the maximum transmission unit (MTU) size to 1492 bytes to allow for the eight additional header bytes used by the PPP and PPPoE encapsulation.
Step 6	**keepalive** *period* [*retries*] **Example:** `Router(config-if)# keepalive 60 10` **Example:** `Router(config-if)#`	(Optional) Specifies how often and how many times the router should send keepalive messages on the virtual interface without receiving a response before bringing down the tunnel protocol and ending that particular PPPoE session. • *period* = Specifies how long, in seconds, the router should send a keepalive message and wait for a response. The valid range is 0 to 32767 seconds, with a default of 10. • *retries* = (Optional) Specifies the number of times the router will resend a keepalive packet without receiving a response. The valid range is 1 to 255, with a default of 5. **Note** Increasing the keepalive period and number of retries might be necessary when supporting a large number of PPPoE sessions.
Step 7	**peer default ip address pool** *name* [*name2 ...*] **Example:** `Router(config-if)# peer default ip address pool local`	(Optional) Defines one or more pools of addresses to be used when assigning IP addresses to the PPPoE clients.

	Command or Action	Purpose
	Example: `Router(config-if)#`	
Step 8	**ppp authentication** {**chap** | **ms-chap** | **pap**} **Example:** `Router(config-if)# ppp authentication chap` **Example:** `Router(config-if)#`	Defines the authentication method to be used for PPPoE sessions: • **chap** = Challenge Handshake Authentication Protocol • **ms-chap** = Microsoft's version of CHAP • **pap** = Password Authentication Protocol
Step 9	**ppp timeout authentication** *response-time* **Example:** `Router(config-if)# ppp timeout authentication 10` **Example:** `Router(config-if)#`	(Optional) Specifies the maximum time, in seconds, that the router should wait for a response to a PPP authentication packet. The valid range is 0 to 255 seconds, with a default of 10 seconds. **Note** Increase this timeout if PPPoE sessions begin failing due to timeout errors.
Step 10	**ppp timeout retry** *timeout* **Example:** `Router(config-if)# ppp timeout retry 5` **Example:** `Router(config-if)#`	(Optional) Specifies the maximum time, in seconds, that the router should wait for a response during PPP negotiation. The valid range is 1 to 255 seconds, with a default of 2 seconds. **Note** Increase this timeout if PPPoE sessions begin failing due to timeout errors.
Step 11	**no logging event link-status** **Example:** `Router(config-if)# no logging event link-status` **Example:** `Router(config-if)#`	(Optional) Disables sending unnecessary link up and link down event messages to the router's event log. These messages would otherwise be sent each time a PPPoE session begins and ends.
Step 12	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	(Optional) Disables the use of the Cisco Discovery Protocol (CDP) on the virtual interface. This protocol is unnecessary on a virtual interface for PPPoE sessions.

	Command or Action	Purpose
	Example: `Router(config-if)#`	
Step 13	**exit** **Example:** `Router(config-if)# exit` **Example:** `Router(config)#`	Exits interface configuration mode.
Step 14	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Configuring a VPDN Group for PPPoE Sessions

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). The router uses the VPDN group to configure the PPPoE sessions it creates for cable modem users. This step is required on the Cisco CMTS.

Note You can create only one VPDN group to support PPPoE sessions.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1` **Example:** `Router(config-vpdn)#`	Creates a VPDN group with the specified name or number and enters VPDN-group configuration mode.
Step 4	Router(config-vpdn)# **accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin` **Example:** `Router(config-vpdn-acc-in)#`	Configures the router to accept tunneled PPP/PPPoE connections from the LAC and enters VPDN accept dialin configuration mode.
Step 5	Router(config-vpdn)# **protocol pppoe** **Example:** `Router(config-vpdn)# protocol pppoe` **Example:** `Router(config-vpdn-acc-in)#`	Configures the VPDN group to use the PPPoE protocol.
Step 6	**virtual-template** *number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1` **Example:** `Router(config-vpdn-acc-in)#`	Specifies the number of the virtual-interface template to be used when configuring a PPPoE session. **Note** This should be the same virtual-interface template defined in Configuring a Virtual Template on the Cisco CMTS, on page 1039.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit` **Example:** `Router(config-vpdn)#`	Exits VPDN accept dialin configuration mode.
Step 8	**lcp renegotiation** {**always** | **on-mismatch**} **Example:** `Router(config-vpdn)# lcp renegotiation always` **Example:** `Router(config-vpdn)#`	(Optional) Specifies whether the Cisco CMTS, acting as the LNS, can renegotiate the PPP Link Control Protocol (LCP) with the router acting as the LAC: • **always** = Always allows the Cisco CMTS to renegotiate the connection. • **on-mismatch** = The Cisco CMTS can renegotiate the connection only when a configuration mismatch is discovered between the LNS and LAC. The default is that the LNS should not be able to renegotiate the connection.
Step 9	**pppoe limit per-mac** *number* **Example:** `Router(config-vpdn)# pppoe limit per-mac 1` **Example:** `Router(config-vpdn)#`	(Optional) Specifies the maximum number of PPPoE sessions that can originate from each MAC address. The valid range is 1 to 5000, with a default of 100. For cable users, Cisco recommends a maximum of 1 PPPoE session per MAC address. **Note** This command is not available until after you have configured the group for the PPPoE protocol in Step 5.
Step 10	**pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number*] **Example:** `Router(config-vpdn)# pppoe limit max-sessions 1000 threshold-sessions 750` **Example:** `Router(config-vpdn)#`	(Optional) Specifies the number of PPPoE sessions supported on the router: • *number* = Specifies the maximum number of PPPoE sessions that can be established at any one time on the router. The valid range is 1 to 5000, with a default of 100. • **threshold-sessions** *number* = (Optional) Specifies the threshold for active PPPoE sessions. If the number of sessions exceeds this value, an SNMP trap can be sent. The valid range is 1 to 5000, and the default equals the *number-of-sessions* value. **Note** This command is not available until after you have configured the group for the PPPoE protocol in Step 5 .

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-vpdn)# exit` **Example:** `Router(config)#`	Exits VPDN-group configuration mode.
Step 12	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting as a when it is acting an L2TP access concentrator (LAC), so that it can create an L2TP tunnel with the L2TP network server (LNS).

Note This step is required when you are using L2TP tunneling with PPPoE sessions. In this configuration, you must create at least one VPDN group to support the PPPoE sessions and at least one other VPDN group to support the L2TP tunnel.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**vpdn-group** *number* **Example:** `Router(config)# vpdn-group 2` **Example:** `Router(config-vpdn)#`	Creates the VPDN group with the specified number and enters VPDN-group configuration mode.
Step 4	Router(config-vpdn)# **request-dialin** **Example:** `Router(config-vpdn)# request-dialin` **Example:** `Router(config-vpdn-req-in)#`	Configures the router to initiate L2TP tunnel requests and enters VPDN request dialin configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp` **Example:** `Router(config-vpdn-req-in)#`	Configures the VPDN group for the L2TP protocol.
Step 6	**domain** *domain-name* **Example:** `Router(config-vpdn-req-in)# domain client.com` **Example:** `Router(config-vpdn-req-in)#`	Specifies that this VPDN group should be used to create PPPoE sessions for clients requesting access from the specified domain name.
Step 7	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits VPDN request dialin configuration mode.

	Command or Action	Purpose
	Example: `Router(config-vpdn)#`	
Step 8	**initiate-to ip** *ip-address* **Example:** `Router(config-vpdn)# initiate-to ip 10.10.10.2` **Example:** `Router(config-vpdn)#`	Establishes the IP address for the termination point of the L2TP tunnel that is used by PPPoE clients using this VPDN group.
Step 9	**local name** *pppoe-username* **Example:** `Router(config-vpdn)# local name PpPoE-UsER` **Example:** `Router(config-vpdn)#`	Specifies the username to be used for authentication on the VPDN group.
Step 10	**no l2tp tunnel authentication** **Example:** `Router(config-vpdn)# no l2tp tunnel authentication` **Example:** `Router(config-vpdn)#`	Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).
Step 11	**exit** **Example:** `Router(config-vpdn)# exit` **Example:** `Router(config)#`	Exits VPDN-group configuration mode.
Step 12	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Enabling PPPoE on a Cable Interface

Use the following commands, starting in user EXEC mode, to enable PPPoE on a specific cable interface on the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0` **Example:** `Router(config-if)#`	Enters cable interface configuration mode for the specified cable interface:
Step 4	**pppoe enable** **Example:** `Router(config-if)# pppoe enable` **Example:** `Router(config-if)#`	Enables PPPoE on the interface, allowing PPPoE sessions to be created through that interface. (The **pppoe enable** command is not available until you enable VPDN operations, using the **vpdn enable** command as shown in the procedure given in the Enabling VPDN Operations on the Cisco CMTS, on page 1037.) **Note** Enabling PPPoE on a cable interface also automatically enables it on all subinterfaces.

	Command or Action	Purpose
Step 5	**hold-queue** *n* **in** **Example:** `Router(config-if)# hold-queue 1000 in` **Example:** `Router(config-if)#`	(Optional) Specify the maximum number of data packets that can be stored in the input queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 75. **Note** To support a large number of simultaneous PPPoE sessions, set the input queue value to at least 1000 packets to avoid dropped packets.
Step 6	**hold-queue** *n* **out** **Example:** `Router(config-if)# hold-queue 1000 out` **Example:** `Router(config-if)#`	(Optional) Specify the maximum number of data packets that can be stored in the output queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 40. **Note** To support a large number of simultaneous PPPoE sessions, set the output queue value to at least 1000 packets to avoid dropped packets. **Note** Repeat Step 3 through Step 6 for each cable interface that supports PPPoE sessions.
Step 7	**exit** **Example:** `Router(config-if)# exit` **Example:** `Router(config)#`	Exits interface configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Configuring a Cisco Router as LNS

Use the following commands, starting in user EXEC mode, to enable and configure a Cisco router, such as the Cisco 6400, to act as the L2TP network server (LNS), so that it can terminate the L2TP tunnels initiated by the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

Note Before performing this procedure on the LNS router, you must also enable VPDN operations, using the procedure given in the Enabling VPDN Operations on the Cisco CMTS, on page 1037. In addition, you must also create and configure a virtual-interface template, using the procedure given in the Configuring a Virtual Template on the Cisco CMTS, on page 1039.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**vpdn-group** *number* **Example:** `Router(config)# vpdn-group 1` **Example:** `Router(config-vpdn)#`	Select the VPDN group number and enters VPDN-group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin` **Example:** `Router(config-config-vpdn-acc-in)#`	Configures the router to accept dial-in calls and enters VPDN accept dialin configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol pppoe`	Configures the VPDN group for the L2TP protocol so that it can access the PPPoE server.

	Command or Action	Purpose
	Example: `Router(config-vpdn-acc-in)#`	
Step 6	**virtual-template** *number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1` **Example:** `Router(config-vpdn-acc-in)#`	Specifies the number of the virtual-interface template to be used when configuring a PPPoE session. **Note** Specify the number of a virtual-interface template that has been created using the procedure given in the Configuring a Virtual Template on the Cisco CMTS, on page 1039.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit` **Example:** `Router(config-vpdn)#`	Exits VPDN accept dialin configuration mode.
Step 8	**terminate-from hostname** *hostname* **Example:** `Router(config-vpdn)# terminate-from hostname ciscocmts-router` **Example:** `Router(config-vpdn)#`	Configures this group so that it terminates L2TP tunnels from the specified hostname. The *hostname* should be the host name for the Cisco CMTS that is configured for PPPoE termination.
Step 9	**no l2tp tunnel authentication** **Example:** `Router(config-vpdn)# no l2tp tunnel authentication` **Example:** `Router(config-vpdn)#`	Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN-group configuration mode.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 11	**virtual-template** *number* **pre-clone** *number* **Example:** `Router(config)# virtual-template 1 pre-clone 2000` **Example:** `Router(config)#`	(Optional) Creates the specified number of virtual interfaces in advance, which can speed up the bring up of individual sessions and reduce the load on the router's processor when a large number of sessions come online at the same time. • *number* = Number of virtual interfaces to be created in advance. This value should match the total number of PPPoE sessions that the router is expected to support. **Note** Pre-cloning is not recommended when using virtual subinterfaces.
Step 12	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Clearing PPPoE Sessions

To clear all PPPoE sessions for a particular MAC address, use the **clear cable host** command:

```
Router# clear cable host
 mac-address

Router#
```

The following example shows a PPPoE session for a particular host being cleared:

```
Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303
1     00         host      offline                     pppoe     0010.2937.b254
Router# clear cable host 0010.2937.b254

Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303
Router#
```

Enabling SNMP Traps for Active PPPoE Sessions

In Cisco IOS Release 12.2(8)BC1 and later releases, you can enable SNMP traps to inform you when the number of active PPPoE sessions exceeds a threshold value, using the following procedure.

Note Configure the threshold value using the **threshold-sessions** option for the **pppoe limit max-sessions** command when configuring the VPDN group for PPPoE sessions. For more information about PPPoE traps, see the CISCO-PPPOE-MIB.

Note To enable SNMP traps, you must also configure the router to support SNMP sessions and specify at least one SNMP manager to receive the SNMP traps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe` **Example:** `Router(config)#`	Enables SNMP traps to be sent whenever the number of active sessions exceeds a user-configurable threshold.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose
	Example: `Router#`	

Monitoring the PPPoE Termination Feature

To display users who have registered with the Cisco CMTS using PPPoE, use the **show interface cable modem** command. For information on this command, see the *Cisco CMTS Cable Command Reference* here

To display the virtual-template interface number being used by a PPPoE client, use the **show vpdn session** command.

```
Router# show vpdn session

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions
34854 14116 R7732-07-ISP1 est    135.1.1.1       1701  1
LocID RemID TunID Intf          Username              State  Last Chg Fastswitch
2     56    34854 Vi1           ppp1@isp1.com         est    00:02:11 enabled
%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
Session count: 1
PPPoE Session Information
SID       RemMAC          LocMAC       Intf     VASt  OIntf         VLAN/
                                                                     VP/VC
1      0050.da80.c13e  0005.00e0.8c8b  Vi1      UP    Ca8/0/1
Router#
```

To display the current VPDN domains, use the **show vpdn domain** command:

```
Router# show vpdn domain
Tunnel          VPDN Group
------          ----------
domain:isp1.com 2 (L2TP)
Router#
```

Configuration Examples for PPPoE Termination

This section lists the following sample configurations for the PPPoE Termination feature:

PPPoE Termination on a Cisco CMTS without L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic from the cable modem users is then sent out over the router's WAN interfaces as IP packets, allowing basic Internet access.

```
version 12.2
!
```

```
hostname ubr-pppoe
!
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! “pppoe enable” command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
 interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
```

```
 no cdp enable
!
```

PPPoE Termination on a Cisco CMTS with L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic received from the cable modem users is sent over the L2TP tunnel to the router that is acting as the L2TP Network Server (LNS).

```
version 12.2
!
hostname ubr-pppoe-l2tp
!
! User name/password sent to LNS to create the L2TP tunnel.
username cmts-user password 0 cmts-password
! User name/password used by LNS to authenticate tunnel creation
username lns-user password 0 lns-password
! User name/password for a PPPoE user - typically this information
! is configured on the RADIUS authentication servers.
username pppoe-user@client.com password 0 user-password
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! VPDN group 2 configures the group to be used for the L2TP tunnel to the
! LNS (at the IP address of 10.10.15.2) which will be used for PPPoE
! sessions from clients using the domain name as "client.com".
vpdn-group 2
 request-dialin
  protocol l2tp
  domain client.com
 initiate-to ip 10.10.15.2
local name ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! “pppoe enable” command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
```

```
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
 no cdp enable
```

PPPoE Client Configuration on a Cisco Router

The following configuration configures a Cisco router that supports PPPoE to act as a PPPoE client. This router connects to the cable modem and performs the PPPoE authentication with the Cisco CMTS that is performing the PPPoE termination.

Note This configuration is for the Cisco 1600 router and needs to be adjusted to fit the interfaces that might be present on other types of routers.

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
!
interface Ethernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp chap hostname joeuser@client.com
 ppp chap password 7 12139CA0C041104
!
```

```
ip nat inside source list 1 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 permit any
```

PPPoE Configuration for the L2TP Network Server

The following sample configuration shows a Cisco router being configured to act as the L2TP Network Server (LNS). This router terminates the L2TP tunnel from the Cisco CMTS and forwards the traffic from the PPPoE sessions to the corporate network.

```
!
hostname lns-router
!
! User name/password for the LNS itself
username lns-user password 0 lns-password
! User name/password for the Cisco CMTS
username cmts-user password 0 cmts-password
! Username and password for the PPPoE client - typically this information is
! configured on the RADIUS authentication servers
username pppoe-user@client.com password 0 user-password
!
ip subnet-zero
ip cef
ip domain-name client.com
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Allows the LNS to preconfigure virtual templates
! for the PPPoE sessions, allowing the sessions to come up faster
virtual-template 1 pre-clone 2000
!
interface loopback 0
ip address 9.10.7.1 255.255.255.0
!
!
interface Virtual-Template1
 ip unnumbered loopback 0
 ip mroute-cache
 ip mtu 1492
 peer default ip address pool pool-1 pool-2
!
ip local pool pool-1 9.10.7.3 9.10.7.254
ip local pool pool-2 9.10.8.1 9.10.8.254
```

Additional References

For additional information related to configuring PPPoE Termination on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring PPP over Ethernet	Configuring Broadband Access: PPP and Routed Bridge Encapsulation, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2, at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/12_2/wan/configuration/guide/fwan_c/wcfppp.html
Enabling SNMP Traps for PPPoE Active Sessions	*PPPoE Session-Count MIB* , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftpscmib.htm
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference Guide,* at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-installation-and-configuration-guides-list.html

Standards

Standards[65]	Title
SP-RFIv1.1-I08-020301	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

65 Not all supported standards are listed.

MIBs

MIBs[66]	MIBs Link
CISCO-PPPOE-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

66 Not all supported MIBs are listed.

RFCs

RFCs[67]	Title
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting

67 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PPPoE Termination

Feature History	
Release	Modification
Release 12.1(5)T	This feature was introduced for the Cisco uBR7200 series routers. **Note** The Cisco IOS Release 12.1T and 12.2T trains are no longer supported for the Cisco uBR7200 series routers.
Release 12.2(4)BC1a	This feature was supported on the 12.2BC train for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
Release 12.2(8)BC1	Support was added for SNMP support with the CISCO-PPPOE-MIB.
Release 12.2(8)BC2	Support was added for bundled cable interfaces.

Feature History
Supported Platforms
Cisco uBR7100 series, Cisco uBR7246VXR router

Note The PPPoE Termination feature is not supported on the Cisco uBR10012 universal broadband router in any Cisco IOS software release. The PPPoE Termination is also not supported on any Cisco CMTS router when running Cisco IOS Release 12.1 EC. Effective with Cisco IOS Release 12.2(33)SCD, the PPPoE Termination feature is not supported on the Cisco uBR7200 router.

CHAPTER 40

Service Flow Mapping to MPLS-VPN on the Cisco CMTS

First Published: February 14, 2008Last Updated: July 11, 2012

This document describes the Service Flow Mapping to MPLS-VPN feature, which enhances the existing multiprotocol label switching (MPLS) VPNs support to provide more flexible managed access for multiple ISP support over a hybrid fiber-coaxial (HFC) cable network.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Mapping Service Flows to MPLS-VPN

- To support static service-flow to MPLS-VPN functionality, the Cisco uBR7200 series routers must be running Cisco IOS Release 12.2(11)BC2 or later releases and the Cisco uBR10000 series routers must be running Cisco IOS Release 12.3(13)BC or later releases.
- To support dynamic service-flow to MPLS-VPN functionality, the Cisco CMTS routers must be running Cisco IOS Release 12.3(13)BC or later releases.
- All Cisco CMTSes must be configured for the proper virtual routing and forwarding (VRF) interfaces, as specified by the documentation in the Additional References, on page 1084.
- To support static service-flow to MPLS VPN mapping, the DOCSIS configuration file editor must support the inclusion of Vendor-specific Options (TLV subtype 43) in the Upstream Service Flow Encodings parameter set (TLV type 24). The new option to be added is called the VPN Route Distinguisher (RD) parameter (TLV subtype 4) and must be preceded by the Cisco Vendor ID (00000C).

For example, using the Cisco DOCSIS Configurator tool, you would specify the following fields in the ASCII configuration file:

```
24 (Upstream Service Flow Block)
  S43 (Vendor Specific Options)
   T08 (Vendor ID) = 00 00 0c
   T04 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
```

where the VPN RD contains eight hexadecimal bytes. The first two hexadecimal bytes specify the format of the remaining six bytes:

- ◦ If bytes 1 and 2 are 00 00, bytes 3 and 4 specify the 16-bit autonomous system (AS) number, and bytes 5 to 8 specify a unique 32-bit identifier.
  ◦ If bytes 1 and 2 are 00 01, bytes 3 to 6 specify the 32-bit IP address, and bytes 7 and 8 specify a unique 16-bit identifier.

Configure the VPN RD parameter to the same *route-distinguisher* ID that you have specified on the Cisco CMTS using the **rd** command in VRF configuration submode.

- To support DOCSIS configuration file-based dynamic service-flow to MPLS VPN mapping, the DOCSIS configuration file editor must support the inclusion of the Cisco Vendor-specific Dynamic Flow VPN RD parameter (TLV subtype 13).

For example, using the Cisco DOCSIS Configurator tool, you would specify the following fields in the ASCII configuration file:

```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = xx xx xx xx xx xx xx xx
```

where the eight-byte VPN RD uses the same format as specified above.

The table shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 109: Service Flow Mapping to MPLS-VPN Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [68]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [69]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V

68 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

69 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Note The combination of a PRE4 and Cisco Half-Height Gigabit Ethernet (HHGE) is not supported in the same chassis.

Restrictions for Mapping Service Flows to MPLS-VPN

- Cable modems using this feature should use a unique DOCSIS configuration file that creates an upstream packet classifier and service flow corresponding to each customer premises equipment (CPE) or media terminal adapter (MTA) device that needs to have its traffic routed to a different MPLS VPN than to the one the cable modem natively belongs.
- The DOCSIS configuration file for a cable modem must be updated whenever a CPE device that needs to use a different MPLS VPN than the cable modem's native MPLS VPN is added or removed, or whenever the MAC address for a CPE device changes. The cable modem must also be reset to execute the changes in the DOCSIS configuration file.
- By default, dynamically generated upstream service flows use the MPLS VPN with which a cable modem is natively associated. In order to specify a different MPLS VPN for use by dynamically generated upstream service flows, it is necessary to do one of the following:
  - Specify an RD in the Cisco Vendor-specific Info Subtype Option 13 within the cable modem's DOCSIS configuration file.
  - Use the global or cable interface command **cable dynamic-flow vrf** to specify an MPLS VPN name.

Information About Mapping Service Flows to MPLS-VPN

The Service Flow Mapping to MPLS-VPN feature provides the following benefits to cable service providers and their partners and customers:

- Allows the service provider to maintain full control over the cable modems and other devices that are directly connected to the cable plant.
- Provides a highly flexible, scalable, and easy to manage system.
- Supports overlapping IP address ranges.
- Provides secure support for multiple intranets and extranets.
- Supports multiple IP Quality of Service (QoS) classes.
- Enables the Cisco CMTS router to support the mapping of dynamic service flows to an MPLS VPN by using the **cable dynamic-flow vrf** command, or the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13) in a DOCSIS configuration file.

The Cisco CMTS routers provide managed access by means of MPLS VPNs configured over cable subinterfaces, with each subinterface configured for a specific ISP and each cable modem associating itself and all connected CPE to a specific subinterface. This use of MPLS VPNs gives service providers a manageable way to offer users access to multiple ISPs over the same physical HFC cable network.

This system works very well when all 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.

As another example, a service provider offering a PacketCable voice-over-IP (VoIP) service may wish to allow one ISP to manage and operate the voice component of the cable network, and another to manage and operate the data component.

The Service Flow Mapping to MPLS-VPN feature solves this problem by using DOCSIS 1.1 upstream packet classifiers and service flow IDs (SFIDs) to map individual CPE devices to separate MPLS-VPN interfaces. The SFID to MPLS-VPN mapping occurs as follows:

1 The service provider creates for each cable modem a DOCSIS configuration file that contains the following information:

   - Secondary upstream service flows that specify QoS profiles for CPE devices that must be associated with a particular MPLS VPN where that MPLS VPN is different from the cable modem's native MPLS VPN assignment.
   - For each upstream service flow, a Vendor-specific QoS Parameter (TLV type 43, subtype 04) that identifies the MPLS VPN RD for packets using this particular service flow.
   - Upstream packet classifiers that correspond to the secondary upstream service flows, so that the cable modem may direct packets from the CPE in question to the correct service flows. To accomplish this, each classifier must contain the MAC address of CPE that are to be associated with the service flow and consequently with the MPLS VPN. This would typically be accomplished by making use of the Source MAC Address parameter (TLV type 10, subtype 2).

Note The DOCSIS configuration file also must create a primary downstream (DS) and a primary upstream (US) service flow and packet classifier, as well as other required parameters, but these are not used for the SFID to MPLS-VPN mapping.

2 The cable modem downloads the DOCSIS configuration file during its registration process and configures itself for the proper service flows and packet classifiers.

3 The cable modem then comes online, at which point 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 CMTS using this upstream SFID.

4 The Cisco CMTS 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.

5 When a dynamic upstream service flow is generated, as in the case with a PacketCable VoIP phone call, the Cisco CMTS determines the MPLS VPN to associate the new upstream service flow by one of several methods in the following order of precedence:

   a If the cable modem's DOCSIS configuration file contains the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13), then the dynamic service flow's VPN is set to the one using the RD as specified in the parameter.

   b If the cable interface on which the modem is online has had the **cable dynamic-flow vrf** command applied, then the dynamic service flow's VPN is set to the MPLS VPN specified by that command.

c If the global **cable dynamic-flow vrf** command is applied, then the dynamic service flow's VPN is set to the MPLS VPN specified by this command.

d Finally, the dynamic service flow's VPN is set to the VPN to which the cable modem is associated.

If the DOCSIS configuration file for the cable modem does not contain an MPLS-VPN route, the packets from that cable modem are routed according to the routing tables on the Cisco CMTS.

MPLS QoS via TLV for non-L2VPN Service Flow

The MPLS QoS via TLV for non-L2VPN Service Flow feature is a QoS enhancement based on MPLS Traffic Class (TC) bits for MPLS L3VPN. This feature is introduced in Cisco IOS Release 12.2(33)SCG to mark TC bits for MPLS L3VPN imposition packets and classify DS packets based on TC bits of MPLS disposition packets, using vendor-specific TLVs.

The MPLS TC bits were previously known as MPLS EXP bits. RFC 5462 has renamed the MPLS EXP field to MPLS TC field.

VoIP SFID Mapping

The introduction of WB MTAs and the resequencing delays with the DS bonded traffic are pushing voice traffic towards non-bonded channels.

Starting with Cisco IOS Release 12.2(33)SCB, as the WB MTA uses the cable interface line card (CLC) DS interface as the primary interface, it can also protect voice traffic from edge quadrature amplitude modulation (e-QAM) and shared port adapter (SPA) failures. It also helps in leveraging the CLC redundancy feature to protect voice calls.

The VoIP Service Flow ID (SFID) Mapping feature leverages Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 Service Flow (SF) Attribute-based assignment, which allows forwarding to Bonding groups or to single channel on a per-SF basis.

The CPE constructs DSX (Dynamic-service DOCSIS mac-management) messages that does not conform to DOCSIS 3.0 specifications and does not includes the SF Attribute parameters. However, the Cisco CMTS should control these factors and whenever voice calls are initiated; the Cisco CMTS must add SF Attributes, configured by the user, to the DSX messages.

Prerequisites for VOIP SFID Mapping

- DOCSIS 3.0-compatible voice CPE and DOCSIS 3.0-compatible PacketCable specifications.
- The Required Attribute Mask and Forbidden Attribute Mask should be configured globally.
- Mask values above zero must be inserted to all dynamic voice DS requests from WB CMs.
- The SF assignment must follow the mask values inserted in DSX message to determine forwarding.
- The Type-Length-Values (TLVs) inserted at the Required Attribute Mask and Forbidden Attribute Mask should not be sent back. They are not supported while sending Dynamic Service Response (DSx-RSP) through embedded media terminal adapter (eMTA) and could lead to cable modem (CM) error.

Restrictions for VOIP SFID Mapping

- The VoIP SFID Mapping feature is supported only on the Cisco uBR10012 Universal Broadband Router.

• DS SF Attribute TLVs inserted by the Cisco CMTS are skipped from TLV encoding.

How to Configure the Service Flow Mapping to MPLS-VPN feature

The following section provides information on how to configure the Service Flow Mapping to MPLS-VPN feature. Each task in the list is identified as either required or optional.

Note This section describes only the configuration tasks needed to enable the Service Flow Mapping to MPLS-VPN feature. It does not describe the basic MPLS-VPN configuration tasks. For information on configuring MPLS-VPN routes, see the documentation listed in the Additional References, on page 1084.

Creating a DOCSIS Configuration File

The Cisco CMTS automatically maps service flows to MPLS-VPN interfaces when an upstream service flow includes the VPN RD parameter as a vendor-specific TLV. The VPN RD parameter points to the *route-distinguisher* ID that has been specified using the **rd** command in VRF configuration submode.

You must create a corresponding upstream packet classifier that identifies the source MAC address that will use this SFID-to-MPLS VPN mapping. To create a DOCSIS configuration file that contains both of these parameters, use the following procedure.

Note This procedure uses the Cisco DOCSIS Configurator tool to create the DOCSIS configuration file. However, you can use any tool that creates DOCSIS-compatible configuration files.

Note For information about the **rd** command, see the command reference.

Step 1 Obtain the MAC addresses for the CPE devices that must be associated with a different MPLS VPN than the cable modem's native MPLS VPN association.

Step 2 Create an upstream packet classifier for each CPE device, specifying the service flow reference of the appropriate upstream service flow and the source MAC address of the CPE, along with the other appropriate parameters. For example, the following configuration for classifier 14 specifies that the service flow with service flow reference 7 should be used for the MAC address at 00 00 0C A1 B2 C3:

Example:

```
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 14
   S03 (Service Flow Reference)         = 7
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 C3
```

Step 3 Create a matching upstream service flow for this CPE device. This service flow must include all necessary parameters, as well as a vendor-specific VPN RD parameter (TLV subtype 4) that identifies the route-distinguisher ID for the VRF route that has been created for this user.

The route-distinguisher ID consists of two integers that can be in the following two forms:

- Type 0—Contains a 16-bit autonomous system (AS) number and a unique 32-bit identifier.
- Type 1—Contains a 32-bit IP address and a unique 16-bit identifier.

Configure the VPN RD parameter to the same *route-distinguisher* ID that you have specified on the Cisco CMTS using the **rd** command in VRF configuration submode. For example, if you configured a type 0 route using the following CLI commands:

Example:

```
ip vrf isp1
 rd 64000:1
```

Configure the matching upstream service flow with the following parameters:

Example:

```
24 (Upstream Service Flow Encodings)
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.250.0.0.0.0.1
```

The Vendor-specific Options field translates into two TLVs. The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C hexadecimal to identify Cisco Systems. The second TLV is of type 4 (VPN RD), length 8, and value of 00.00.FA.0.0.0.0.1 (hexadecimal).

Tip If you are using the graphical interface in the Cisco DOCSIS Configurator tool to create the DOCSIS configuration file, enter the entire dotted decimal string into the "Vendor Specific QoS" field in the Upstream and Downstream Service Flow screens. Using the above example, you would enter "8.3.0.0.12.4.8.0.0.0.250.0.0.0.1" into this field.

Similarly, if you configured a type 1 route using the following CLI commands:

Example:

```
ip vrf isp2
 rd 10.10.10.15:1
```

Configure the matching upstream service flow with the following parameters:

Example:

```
24 (Upstream Service Flow Encodings)
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.1.10.10.10.15.0.1
```

Similarly, the Vendor-specific Options field translates into two TLVs. The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C hexadecimal to identify Cisco Systems. The second TLV is of type 4 (VPN RD), length 8, and value of 00.01.0A.0A.0A.0F.00.01 (hexadecimal).

Step 4 Repeat this procedure for each upstream packet classifier and service flow that is to be mapped to an MPLS-VPN interface.

Mapping Dynamic Service Flows

If the MPLS VPN to which dynamic service flows are mapped must be set on a per-cable-modem basis, rather than on a per-cable-interface or per-Cisco-CMTS basis, then the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13) must be added to the DOCSIS configuration. The Dynamic Flow VPN RD parameter is used to specify the route-distinguisher ID for the VRF route that has been created for use by dynamic service flows.

Note In general, the MPLS VPN to which dynamic service flows must be mapped should be the same MPLS VPN as specified for static service-flow to MPLS VPN mapping.

Step 1 Refer to Step 3 of Creating a DOCSIS Configuration File, on page 1069.

Step 2 Configure the VPN RD parameter to the same route-distinguisher ID that you have specified on the Cisco CMTS by means of the **rd** command in VRF configuration submode. For example, if you configured a type 0 route by means of the following CLI commands:

Example:
```
ip vrf isp1
rd 64000:1
```

Configure the matching Dynamic Flow VPN RD parameter as follows:

Example:
```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-0-fa-0-0-0-0-1
```

The Vendor-specific Options field translates into two TLVs:

- The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C (hexadecimal), to identify Cisco Systems.
- The second TLV is of type 4 (VPN RD), length 8, and value of 00.00.FA.0.0.0.0.1 (hexadecimal).

Similarly, if you configured a type 1 route by means of the following CLI commands:

Example:
```
ip vrf isp2
rd 10.10.10.15:1
```

Configure the matching upstream service flow with the following parameters:

Example:
```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-1-a-a-a-f-0-1
```

Similarly, the Vendor-specific Options field translates into two TLVs:

- The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C (hexadecimal) to identify Cisco Systems.
- The second TLV is of type 4 (VPN RD), length 8, and value of 00.01.0A.0A.0A.0F.00.01 (hexadecimal).

The per-cable-modem Dynamic Flow VPN RD parameter takes precedence over any per-cable-interface or per-Cisco-CMTS dynamic service flow to MPLS VPN configuration.

Step 3 If the MPLS VPN to which dynamic service flows are mapped must be set on a per-cable-interface basis, as opposed to per cable modem or per-Cisco-CMTS, then use the following the cable interface configuration command:

Example:
```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 vrf-name
```

For example, if you configured the following VRF for use with dynamically generated service flows:

Example:
```
ip vrf isp1
 rd 64000:1
```

Then you could use the following per-cable-interface command to ensure that dynamic service flows are mapped:

Example:
```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 isp1
```

The per-cable-interface dynamic service flow to MPLS VPN configuration takes precedence over the global per-Cisco-CMTS dynamic service flow to MPLS VPN configuration, but not over the per-cable-modem Dynamic Flow VPN RD parameter.

Step 4 If the MPLS VPN to which dynamic service flows are mapped must be set on a per-Cisco-CMTS basis, as opposed to per cable modem or per cable interface, then use the global configuration command:

Example:
```
Router# cable dynamic-flow vrf
 vrf-name
```

For example, if you configured the following VRF for use with dynamically generated service flows:

Example:
```
ip vrf isp2
 rd 10.10.10.15:1
```

Then you could use the following per-cable-interface command to ensure that dynamic service flows are mapped:

Example:

```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 isp2
```

Configuring MPLS QoS via TLV for non-L2VPN Service Flow

Note This feature is configured using a cable modem configuration file and is dependent on the general configuration of the L3VPN.

This section describes how to configure traffic class bits for MPLS imposition and disposition packets and on how to use vendor-specific TLVs with AToM L2VPN and MPLS L3VPN.

Restrictions for Configuring MPLS QoS via TLV

- This feature supports only PRE4. It will not support PRE2.
- This feature supports only IPv4. It will not support IPv6.
- This feature supports only Cisco uBR10012 routers. The Cisco uBR7200 series routers is not supported.
- This feature does not support SNMP.
- This feature does not support dynamic service flows.
- Only up to four VPNs and eight upstream service flows per CM can be configured.
- For a VPN, only a maximum of eight DS classifiers (using TC bits in the range from 0 to 7) can be configured.
- If TC bits downstream classifiers are configured for a VPN, then the downstream MPLS packets belonging to the VPN are processed only on TC bits classification. It will not process general IP header field classification.

Traffic Class for MPLS Imposition Packets

The table lists the vendor-specific TLV to be included in the cable modem configuration file to configure TC bits for MPLS imposition packets. The MPLS-TC-SET TLV is defined in the upstream and is associated with the VPN RD in upstream service flow encoding.

Table 110: TLV to Configure TC Bits for MPLS Imposition Packets

TLV Name	SubType	Length	Value
MPLS-TC-SET TLV	43.5.43.34	1	Imposition MPLS-TC-SET bits

Traffic Classification for MPLS Disposition Packets

The table lists the vendor-specific TLV to be included in the cable modem configuration file to classify DS packets based on TC bits of MPLS disposition packets.

The MPLS-TC-RANGE TLV is defined only under DS classifier encodings. It supports multi-downstream flow in a CM belonging to the same MPLS L3VPN, associated with the VPN RD in downstream classifier encoding.

Table 111: TLV to Classify TC Bits for MPLS Disposition Packets

TLV Name	SubType	Length	Value
MPLS-TC-RANGE	43.5.43.35	2	MPLS-TC-low and MPLS-TC-high

Using Vendor-Specific TLVs with AToM L2VPN and MPLS L3VPN

If both AToM L2VPN (L2 MPLS) and MPLS L3VPN (L3 MPLS) are using the same set of TLVs (MPLS-TC-SET and MPLS-TC-RANGE), then you should differentiate them. Configure the TLVs for upstream service flow encoding and downstream classifier encodings as indicated below:

Upstream Service Flow Encoding

- For L2VPN, configure MPLS-TC-SET (43.5.43.34) and L2VPN ID (43.5.1).
- For MPLS L3VPN, configure MPLS-TC-SET (43.5.43.34) and VPN RD (43.5.1).

Note Do not configure the TLVs for L2VPN and MPLS L3VPN at the same time for upstream service flow encodings, as it will result in a TLV error.

Downstream Classifier Encoding

- L2VPN—Configure MPLS-TC-RANGE (43.5.43.35) and L2VPN ID (43.5.1).
- MPLS L3VPN—Configure MPLS-TC-RANGE (43.5.43.35) and VPN RD (43.5.1).

Monitoring and Maintaining Examples for Service Flow Mapping to MPLS-VPN Feature

This section provides examples of the commands that show the configuration and current status of the cable modems (CMs) that are using the Service Flow Mapping to MPLS-VPN feature. These examples display a number of CMs that are online, and the last CM (with the primary service identifier [SID] of 6) has three CPE devices connected to separate ISPs.

Displaying CMs and CPE devices

To display the number of CMs that are currently registered and online, use the **show cable modem** command:

```
Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0030.8047.b41f 5.108.1.21      C3/0/U2   online(pt)  1    0.75   2821    0   Y
0007.0e03.1349 5.109.1.9       C3/0/U0   online      2   *0.00   2816    0   N
0007.0e03.12bd 5.108.1.18      C3/0/U0   online(pt)  3    -0.25  2812    0   Y
0030.80bc.22d5 5.108.1.20      C3/0/U0   online(pt)  4    0.25   2819    0   Y
0007.0e03.1331 5.111.1.6       C3/0/U0   online      5    -0.25  2816    0   N
00a0.73b0.4cc1 5.110.1.6       C3/0/U0   online(pt)  6    -0.25  2990    3   Y
```

To display the CPE devices that are associated with each CM, use the **show interface cable modem** command:

```
Router# show interface cable 3/0 modem 0

SID   Priv bits  Type      State     IP address      method    MAC address
1     11         modem     up        5.108.1.21      dhcp      0030.8047.b41f
2     00         modem     up        5.109.1.9       dhcp      0007.0e03.1349
3     11         modem     up        5.108.1.18      dhcp      0007.0e03.12bd
4     11         modem     up        5.108.1.20      dhcp      0030.80bc.22d5
5     00         modem     up        5.111.1.6       dhcp      0007.0e03.1331
6     11         modem     up        5.110.1.6       dhcp      00a0.73b0.4cc1
6     11         host      unknown   131.1.2.30      dhcp      0002.e323.ac08
6     11         host      unknown   129.1.2.18      dhcp      0050.046b.8b97
6     11         host      unknown   130.1.2.24      dhcp      0050.da80.c13e
```

To display the MPLS VPN RD to be used by dynamic service flows from a cable modem using the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13), use the **show cable modem verbose** command:

```
Router# show cable modem 0007.0e02.afa5 verbose
MAC Address                     : 00a0.73b0.4cc1
IP Address                      : 5.110.1.6
Prim Sid                        : 6
Interface                       : C3/0/U0
sysDescr                        :
Upstream Power                  : 0.00 dBmV (SNR = 33.83 dB)
Downstream Power                : 0.00 dBmV (SNR = ----- dB)
Timing Offset                   : 2290
Initial Timing Offset           : 2290
Received Power                  :  0.00 dBmV
MAC Version                     : DOC1.1
QoS Provisioned Mode            : DOC1.1
Enable DOCSIS2.0 Mode           : Y
Phy Operating Mode              : tdma
Capabilities                    : {Frag=Y, Concat=Y, PHS=Y, Priv=BPI+}
Sid/Said Limit                  : {Max US Sids=4, Max DS Saids=0}
Optional Filtering Support      : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support      : {Taps/Symbol= 1, Num of Taps= 8}
Number of CPE IPs               : 0(Max CPE IPs = 16)
CFG Max-CPE                     : 5
Flaps                           : 0()
Errors                          : 0 CRCs, 0 HCSes
Stn Mtn Failures                : 0 aborts, 0 exhausted
Total US Flows                  : 1(1 active)
Total DS Flows                  : 1(1 active)
Total US Data                   : 1606 packets, 129106 bytes
Total US Throughput             : 43 bits/sec, 0 packets/sec
Total DS Data                   : 28 packets, 1792 bytes
Total DS Throughput             : 0 bits/sec, 0 packets/sec
Active Classifiers              : 0 (Max = NO LIMIT)
DSA/DSX messages                : permit all
Dynamic Secret                  : 4E7AD0AEA48F94DE0EB773494B57EA74
Dynamic flows mapped to VPN RD  : 64000:1
```

```
! The dynamic mapping is listed above.
Total Time Online                  : 1d3h
```

Displaying SID and MPLS Mappings

To display the mapping of currently used SIDs to SFIDs and their current state, use the **show interface cable sid verbose** command:

```
Router# show interface cable 3/0 sid verbose

Sid  Prim  MAC Address    IP Address      Type Age      Admin   Sched  Sfid
                                                       State   Type
1          0030.8047.b41f 5.108.1.21      stat 3h43m    enable  RSVD   3
2          0007.0e03.1349 5.109.1.9       stat 3h43m    enable  RSVD   5
3          0007.0e03.12bd 5.108.1.18      stat 3h43m    enable  BE     7
4          0030.80bc.22d5 5.108.1.20      stat 3h43m    enable  BE     9
5          0007.0e03.1331 5.111.1.6       stat 3h42m    enable  BE     11
6          00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     13
7    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     15
8    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     16
9    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     17
10   6     00a0.73b0.4cc1 5.110.1.6       dyn  02:35    enable  UGS    18
```

To display the mappings between SFIDs and the MPLS VPN subinterface, use the **show interface cable sid association** command:

```
Router# show interface cable 3/0 sid association

Sid  Prim Online     IP Address      MAC Address    Interface     VRF Name
1         online(pt) 5.108.1.21      0030.8047.b41f Bu1.101       isp1
2         online     5.109.1.9       0007.0e03.1349 Bu1.102       isp2
3         online(pt) 5.108.1.18      0007.0e03.12bd Bu1.101       isp1
4         online(pt) 5.108.1.20      0030.80bc.22d5 Bu1.102       isp1
5         online     5.111.1.6       0007.0e03.1331 Bu1.102       isp2
6         online(pt) 5.110.1.6       00a0.73b0.4cc1 Bu1.103       isp3
7    6                                             Bu1.101       isp1
8    6                                             Bu1.102       isp2
9    6                                             Bu1.103       isp3
10   6                                             Bu1.102       isp2
```

Displaying Service Flow Configurations

To display the basic mapping of service flows and packet classifiers, use the **show interface cable service-flow** command. To display complete service flow configuration information, add the **verbose** keyword.

The following examples display the service flow information for the CM that is using the primary SID of 6 and the SFID of 13:

```
Router# show interface cable 3/0 service-flow 13

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                            Prov  Adm  Act                  State  Time
13    6     00a0.73b0.4cc1   7     7    7     prim    US     act    12:59
```

```
Router# show interface cable 3/0 13 verbose

Sfid                                  : 13
Mac Address                           : 00a0.73b0.4cc1
Type                                  : Primary
Direction                             : Upstream
Current State                         : Active
```

```
Current QoS Indexes [Prov, Adm, Act]    : [7, 7, 7]
Active Time                             : 13:02
Sid                                     : 6
Traffic Priority                        : 0
Maximum Sustained rate                  : 0 bits/sec
Maximum Burst                           : 3044 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 13
Bytes                                   : 1833
Rate Limit Delayed Grants               : 8
Rate Limit Dropped Grants               : 0
Current Throughput                      : 0 bits/sec, 0 packets/sec
Classifiers: NONE
```

The following examples display the service flow information for the first CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 7 and the SFID of 15, and is using the VRF configuration named **isp1**.

```
Router# show interface cable 3/0 15

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                           Prov  Adm  Act                  State  Time
15    7     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    13:33
```

```
Router# show interface cable 3/0 15 verbose

Sfid                                    : 15
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Static)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [8, 8, 8]
Active Time                             : 13:36
Sid                                     : 7
Traffic Priority                        : 0
Maximum Sustained rate                  : 1000000 bits/sec
Maximum Burst                           : 65224 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 0 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 56
Bytes                                   : 8608
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 0 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 1
Service Flow Id                         : 15
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 0
PHSI                                    : 0
Number of matches                       : -
Ethernet/LLC Classifier Parameters      :
Source MAC                              : 0000.0CA1.B2C3
```

The following example displays the service flow information for the second CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 8 and the SFID of 16, and is using the VRF configuration named **isp2**.

```
Router# show interface cable 3/0 service-flow 16

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                           Prov  Adm  Act                  State  Time
```

```
16    8     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    14:04
```

```
Router# show interface cable 3/0 service-flow 16 verbose

Sfid                                    : 16
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Static)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [8, 8, 8]
Active Time                             : 14:08
Sid                                     : 8
Traffic Priority                        : 0
Maximum Sustained rate                  : 1000000 bits/sec
Maximum Burst                           : 65224 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 0 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 155
Bytes                                   : 20418
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 0 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 2
Service Flow Id                         : 16
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 0
PHSI                                    : 0
Number of matches                       : -
Ethernet/LLC Classifier Parameters      :
Source MAC                              : 0000.0CA1.B2D4
```

The following example displays the service flow information for the third CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 9 and the SFID of 17, and is using the VRF configuration named **isp3**.

```
Router# show interface cable 3/0 service-flow 17

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                           Prov  Adm  Act                    State  Time
17    9     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    14:33
```

```
Router# show interface cable 3/0 service-flow 17 verbose

Sfid                                    : 17
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Static)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [8, 8, 8]
Active Time                             : 14:36
Sid                                     : 9
Traffic Priority                        : 0
Maximum Sustained rate                  : 1000000 bits/sec
Maximum Burst                           : 65224 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 0 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 141
Bytes                                   : 16152
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 33 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 3
```

```
Service Flow Id                          : 17
CM Mac Address                           : 00a0.73b0.4cc1
Direction                                : upstream
Activation State                         : active
Classifier Matching Priority             : 0
PHSI                                     : 0
Number of matches                        : -
Ethernet/LLC Classifier Parameters       :
Source MAC                               : 0000.0CA1.B2E5
```

The following example displays the service flow information for a dynamically generated PacketCable service flow on the modem with a primary SID of 6. The dynamic service flow is using a secondary SID of 10 and an SFID of 18, and is using the VRF configuration named isp2.

```
Router# show interface cable 3/0 service-flow 18 verbose
Sfid                                     : 18
Mac Address                              : 00a0.73b0.4cc1
Type                                     : Secondary(Dynamic)
Direction                                : Upstream
Current State                            : Active
Current QoS Indexes [Prov, Adm, Act]     : [0, 5, 5]
Active Time                              : 02:59
Sid                                      : 10
Admitted QoS Timeout                     : 200 seconds
Active QoS Timeout                       : 0 seconds
Packets                                  : 8967
Bytes                                    : 2080344
Rate Limit Delayed Grants                : 0
Rate Limit Dropped Grants                : 0
Current Throughput                       : 92399 bits/sec, 49 packets/sec
Classifiers:
Classifier Id                            : 1
Service Flow Id                          : 18
CM Mac Address                           : 00a0.73b0.4cc1
Direction                                : upstream
Activation State                         : active
Classifier Matching Priority             : 64
PHSI                                     : 0
Number of matches                        : -
IP Classification Parameters             :
IP Source Address                        : 4.22.96.99
Source IP Address Mask                   : 255.255.255.255
Destination IP Address                   : 4.18.39.12
Destination IP Address Mask              : 255.255.255.255
IP Protocol Type                         : 17
Source Port Low                          : 16622
Source Port High                         : 16622
Destination Port Low                     : 17640
Destination Port High                    : 17640
```

Configuration Examples

This section provides the following configuration examples:

Example: DOCSIS Configuration File

The following example shows a cable modem being configured to support three MPLS VPN routes. This includes three upstream packet classifiers and three upstream service-flow parameter sets. It also shows the configuration required to have dynamic service flows associated with a particular MPLS VPN:

```
CM-CONFIG
=========
```

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 100
28 (Max Number of Classifiers)  = 4
29 (Privacy Enable)             = 1
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 10
   S03 (Service Flow Reference)         = 3
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 C3
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 12
   S03 (Service Flow Reference)         = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 D4
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 14
   S03 (Service Flow Reference)         = 7
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 E5
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 3
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.250.0.0.0.0.1
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 5
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.246.24.0.0.0.1
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 7
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.253.232.0.0.0.1
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-0-fa-0-0-0-0-1
#<EOF>
```

Example: MPLS VPN Interface Configuration

The following example shows the corresponding VRF configurations with the three VRF route-designators that match the MPLS-VPN configuration that is used on the cable modem:

```
ip vrf MGMT
 rd 1:1
 route-target export 62000:1
 route-target import 62000:1
 route-target import 63000:1
 route-target import 64000:1
```

```
 route-target import 65000:1
!
ip vrf isp1
 rd 64000:1
 route-target export 64000:1
 route-target import 64000:1
 route-target import 62000:1
!
ip vrf isp2
 rd 63000:1
 route-target export 63000:1
 route-target import 63000:1
 route-target import 62000:1
!
ip vrf isp3
 rd 65000:1
 route-target export 65000:1
 route-target import 65000:1
 route-target import 62000:1
!
interface Bundle1
 no ip address
 hold-queue 1024 in
!
interface Bundle1.100
 ip vrf forwarding MGMT
 ip address 10.22.32.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.101
 ip vrf forwarding isp1
 ip address 10.22.64.1 255.255.224.0
 ip address 4.22.64.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.102
 ip vrf forwarding isp2
 ip address 10.22.96.1 255.255.224.0
 ip address 4.22.96.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.103
 ip vrf forwarding isp3
 ip address 10.22.128.1 255.255.224.0
 ip address 4.22.128.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
```

Example: Upstream Service Flow Marking TLV

The following example shows a sample CM configuration TLV for the provisioning of TC bits for MPLS imposition packets:

```
24 (Upstream Service Flow Encoding)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       T004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
            S005 (Vendor specific L2VPN TLV)
            S043 (Cisco Vendor Specific)
       T034 (MPLS-TC-SET) = 04 # MPLSTC-SET = 4
```

Example: Downstream Packet Classification TLV

The following example shows a sample CM configuration TLV for classifying downstream packets based on TC bits of MPLS disposition packets:

```
23 (Downstream Packet Classification Encoding)
   S01 (Classifier Reference)           = 13
   S03 (Service Flow Reference)         = 13
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       S004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
       S005 (Vendor specific L2VPN TLV)
           S043 (Cisco Vendor Specific)
           S035 (MPLS-TC-RANGE)   = 04  05      # MPLSTC-EGRESS_RANGE= 4 - 5
```

Example: MPLS QoS Configuration File

The following example shows a cable modem being configured to mark TC bits for MPLS L3VPN imposition packets and classify downstream packets based on TC bits of MPLS L3VPN disposition packets, using vendor-specific TLVs:

```
CM-CONFIG
=========
03 (Net Access Control)                      = 1
18 (Maximum Number of CPE)       = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 2
   S03 (Service Flow Reference)        = 2
   S05 (Rule Priority)                             = 2
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 20 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 3
   S03 (Service Flow Reference)        = 3
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 40 80 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 4
   S03 (Service Flow Reference)        = 4
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = a0 e0 ff
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 12
   S03 (Service Flow Reference)        = 12
   S05 (Rule Priority)                             = 2
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 01 01
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 13
   S03 (Service Flow Reference)        = 13
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 02 02
23 (Downstream Packet Classification Encoding Block)
```

```
   S01 (Classifier Reference)              = 14
   S03 (Service Flow Reference)        = 14
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 03 03
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 1
   S06 (QoS Parameter Set Type)     = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 2
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 3
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 4
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 06
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 11
   S06 (QoS Parameter Set Type)     = 7
   S07 (Traffic Priority)                          = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 12
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 13
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 14
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 15
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 16
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 17
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 18
   S06 (QoS Parameter Set Type)     = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 19
   S03 (Service Flow Reference)        = 19
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 00 00
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 15
   S03 (Service Flow Reference)        = 15
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
```

```
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 04 04
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)               = 16
   S03 (Service Flow Reference)         = 16
   S05 (Rule Priority)                              = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)              = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 05 05
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)               = 17
   S03 (Service Flow Reference)         = 17
   S05 (Rule Priority)                              = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)              = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 06 06
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)               = 18
   S03 (Service Flow Reference)         = 18
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)              = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 07 07
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 19
   S06 (QoS Parameter Set Type)     = 7
#<EOF>
```

Additional References

The following sections provide references related to the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference Guide*, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Cisco IOS Release 12.2	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URLs: http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-installation-and-configuration-guides-list.html http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-command-reference-list.html

Related Topic	Document Title
Configuring cable features	*Cisco IOS CMTS Cable Software Configuration Guide* , *Release 12.2SC* , at the following URL: http://www.cisco.com/web/techdoc/cable/Config/Sw_conf.html
Installing and configuring Cisco uBR7200 Series Universal Broadband Routers	Cisco uBR7200 Universal Broadband Routers, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html
Installing and configuring the Cisco uBR10012 Router	Cisco uBR10012 Universal Broadband Router, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/quick/start/10kqsg_2.html
Service provider solution	Cisco Cable-Ready High Speed Data (HSD) Managed Access Solution for Service Providers, at the following URL: http://www.cisco.com/c/en/us/solutions/service-provider/cable-high-speed-data-hsd-solutions/index.html
MPLS VPN	Cisco uBR7200 Series MPLS VPN Cable Enhancements, which is at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/cable/configuration/guide/12_2sc/Cisco_CMTS_Layer2_VPN/u72_mpls_vpn_cbl.html

Standards

Standard	Title
DOCSIS	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification (SP-RFIv1.1-I08-020301)

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 1163	A Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 2233	DOCSIS OSSI Objects Support
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2547	BGP/MPLS VPNs
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB
RFC 5462	Multiprotocol Label Switching (MPLS) Label Stack Entry: “EXP” Field Renamed to “Traffic Class” Field

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

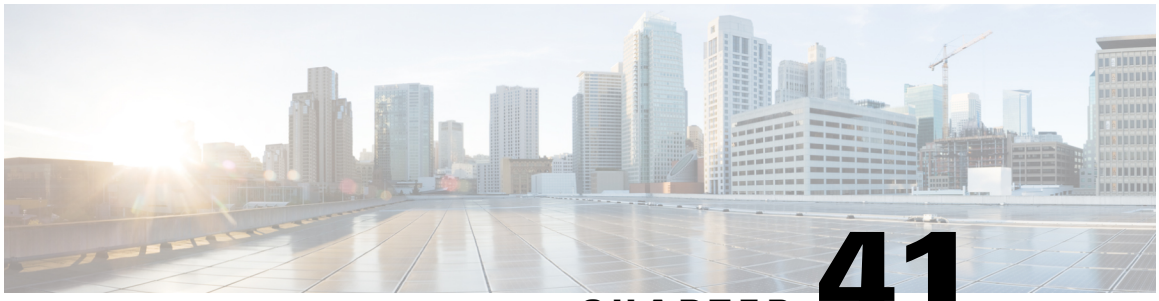
Feature Information for Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 112: Feature Information for Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers	12.2(11)BC2	This feature was supported on the Cisco uBR7100 series and Cisco uBR7200 series universal broadband routers.
Mapping Dynamic Service Flows	12.3(13)BC	Support was added for mapping dynamic service flows on the Cisco uBR7200 series and the Cisco uBR10000 series.
VoIP SFID Mapping	12.2(33)SCB	Support was added for the VoIP SFID Mapping feature.
MPLS QoS via TLV for non-L2VPN SF	12.2(33)SCG	This feature allows to mark TC bits for MPLS L3VPN imposition packets and classify downstream packets based on TC bits of MPLS disposition packets, using vendor-specific TLVs. The following sections provide information about this feature:



CHAPTER 41

Transparent LAN Service over Cable

First Published: February 14, 2008

This document describes the Transparent LAN Service over Cable feature, which 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 IEEE 802.1Q Virtual Local Area Network (VLAN).

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

• Feature Information for Transparent LAN Service over Cable, page 1099

Prerequisites for Transparent LAN Service over Cable

The Transparent LAN Service over Cable feature has the following prerequisites:

- You must know the hardware (MAC) addresses of the cable modems that are to be mapped to IEEE 802.1Q VLANs.
- You must create a bridge group for each separate customer on the Layer 2 bridge aggregator, so that traffic from all of the Customer Premises Equipment (CPE) devices for the customer is grouped together into the same ATM or 802.1Q tunnel.

Restrictions for Transparent LAN Service over Cable

- 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.
- We strongly recommend that TLS over Cable only be used when Baseline Privacy Interface (BPI) is enabled in the environment. If BPI is not enabled when using the TLS feature, traffic can flow between multiple virtual private networks (VPNs), and become vulnerable to denial-of-service attacks or snooping. We also recommend that remote networks be isolated with a gateway or firewall router when BPI is not enabled.

Commencing in Cisco IOS release 12.3(13a)BC, and later releases, 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.

- Packets are mapped to their Layer 2 tunnel only on the basis of Layer 2 information (the cable modem's MAC address and primary SID). Layer 3 services, such as access lists, IP address source-verify, and IP QoS, are not supported as packets are sent through the tunnel.
- All traffic from a cable modem is mapped to the same Layer 2 tunnel. It is not possible to differentiate traffic from different customer premises equipment (CPE) devices behind the cable modem.
- CPE learning is not available when using the Transparent LAN Service over Cable feature. When a cable modem is mapped to a Layer 2 tunnel, the **show interface cable modem** command shows that the IP addresses for its CPE devices are "unavailable."
- DOCSIS QoS is supported across the Layer 2 tunnel only on the primary SID. Traffic using secondary services uses the same Layer 2 tunnel as the primary SID.
- The Spanning Tree Protocol (STP) cannot be used with devices (cable modems, their CPE devices, and the endpoint CPE devices) that are using this feature. In particular, Spanning Tree Protocol cannot be used between the VLAN bridge aggregator and the endpoint customer devices.
- The following restrictions apply to Layer 2 tunnels over an ATM interface:
  - The virtual connections (VC) on the ATM interface must be configured to use ATM Adaptation Layer 5 (AAL5) IEEE 802.1a Subnetwork Access Point (SNAP) encapsulation. On Cisco routers,

this means that each PVC endpoint must be configured for the proper encapsulation using the **encapsulation aal5snap** command.

- The following restrictions apply to Layer 2 tunnels over an Ethernet IEEE 802.1Q VLAN interface:
  - IEEE 802.1Q tunnels are supported only on Ethernet, Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet interfaces.
  - The Cisco CMTS router supports a maximum of 4095 VLAN IDs, but the switches acting as the bridge aggregator might support a lower number of VLAN IDs. If this is the case, the Cisco CMTS should be configured only for the maximum number of VLANs that are supported by the bridge aggregator switches.

Information About Transparent LAN Service over Cable

This section contains the following:

Feature Overview

The Transparent LAN Service over Cable feature enables service providers to provide Layer 2 tunnels for traffic to and from cable modems. This allows customers to create their own virtual local area network (VLAN) using any number of cable modems in multiple sites.

On the Cisco CMTS, you map each cable modem (on the basis of its MAC address) to the appropriate VLAN. The CMTS then creates an internal database of this one-to-one mapping of cable modems to VLANs, and uses it to encapsulate packets for the appropriate VLAN.

The CMTS encapsulates the CPE traffic from mapped cable modems using the following method:

- IEEE 802.1Q Mapping—The cable modem's MAC address is mapped to an IEEE 802.1Q VLAN on a specific Ethernet interface, so that all traffic from the cable modem is tagged with the specified VLAN ID.

Traffic to and from this group of cable modems is bridged into a single logical network (the VLAN) by the bridge aggregator, creating a secure Virtual Private Network (VPN) for that particular group of cable modems. Traffic in one VLAN cannot be sent into another VLAN, unless specifically done so by an external router.

The switch acting as the Layer 2 Bridge Aggregator uses the VLAN tagging to forward the traffic to the appropriate destination. This frees up service providers from needing to know the addressing, routing, and topological details of the customer's network.

Transparent LAN Service and Layer 2 Virtual Private Networks

In addition, service providers can provide a Layer 2 VPN with only minimal configuration changes on the provider's routers. The service subscriber does not need to make any changes to their private network or cable modems, nor does the service provider have to provide any special DOCSIS configuration files to enable this feature.

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.

IEEE 802.1Q Mapping

This section describes the mapping of cable modems to an IEEE 802.1Q VLAN, as it is available in the Transparent LAN Service over Cable feature:

Overview

The Transparent LAN Service over Cable feature enables service providers to provide Layer 2 tunnels over an Ethernet network, using IEEE 802.1Q standard tags. This allows customers to create their own virtual network using any number of cable modems in different sites.

On the Cisco CMTS, you map each cable modem (on the basis of its MAC address) to the appropriate VLAN. The CMTS then creates an internal database of this one-to-one mapping of cable modems to VLANs, and uses it to encapsulate packets for the appropriate VLAN.

The CMTS encapsulates the CPE traffic from mapped cable modems using VLAN tags, as defined in IEEE 802.1Q-1993, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks . The switch acting as the Layer 2 Bridge Aggregator uses the VLAN tagging to forward the packets to the appropriate destination.

Traffic to and from this group of cable modems is bridged into a single logical network by the bridge aggregator, creating a secure Virtual Private Network (VPN) for that particular group of cable modems. Traffic in one VLAN cannot be sent into another VLAN, unless specifically done so by an external router.

Details of IEEE 802.1Q Mapping

To implement the Transparent LAN Service over Cable feature using IEEE 802.1Q VLANs, a service provider must perform the following configuration steps:

1. Identify the cable modems and their MAC addresses that should be mapped to the IEEE 802.1Q VLANs.
2. Create the required VLANs on the router that is acting as the bridge aggregator.
3. Enable Layer 2 mapping on the Cisco CMTS, and then map each cable modem on that Cisco CMTS to the appropriate VLAN.

After the Transparent LAN Service over Cable feature has been enabled and configured to use IEEE 802.1Q mappings, the Cisco CMTS immediately begins mapping traffic between the associated cable modems and VLANs. For efficient mapping, the Cisco CMTS maintains an internal database that links each cable modem's primary service flow ID (SFID) and service ID (SID) to the appropriate VLAN and Ethernet interface. This ensures that all service flows from the cable modem are routed properly.

When the Cisco CMTS receives a packet on an upstream, it looks up its SID to see if it is mapped to a VLAN. If so, and if the packet's source MAC address is not the cable modem's MAC address, the Cisco CMTS inserts the appropriate IEEE 802.1Q VLAN tag into the packet's header and forwards the packet to the appropriate Ethernet interface. If the packet is not being mapped, or if the packet originated from the cable modem, the Cisco CMTS routes the packet using the normal Layer 3 processes.

When the Cisco CMTS receives a packet from a WAN interface that is encapsulated with an IEEE 802.1Q VLAN tag, it looks up the packet's SID to see if it belongs to a cable modem being mapped. If so, the Cisco CMTS strips off the VLAN tag, adds the proper DOCSIS header, and transmits the packet on the appropriate downstream interface. If the packet is not being mapped, the Cisco CMTS continues with the normal Layer 3 processing.

Benefits

The Transparent LAN Service over Cable feature provides the following benefits to cable service providers and their partners and customers:

- Provides Layer 2 level mapping, which is transparent to Layer 3 protocols and services. This means that service providers do not need to know the details of their customers' network topologies, routing protocols, or IP addressing.
- Allows service providers to maximize the use of their existing ATM or Ethernet WAN networks. Multiple customers can be combined on the same outgoing interface, while still ensuring that each customer's network is kept private while it is transmitted over the tunnel.
- Provides a highly flexible and scalable solution for multiple customers. The service provider needs to create only one bridge group for each VPN, and then only one VLAN mapping for each cable modem should participate in that VPN tunnel.
- Customers retain full control over their private networks, while service providers retain full control over cable modems and the rest of the cable and ATM networks. Only the CPE traffic from the cable modems is mapped into the ATM tunnel, while traffic originating at the cable modem continues to be processed as normal by the service provider's network.
- Allows service providers to mix tunneled and non-tunneled cable modems on the same DOCSIS cable network.
- Allows customers to create a single, secure virtual network with Ethernet Layer 2 connectivity for multiple sites.
- Allows multiple tunnels from different customers and endpoints to be aggregated into a single bridge, so as to maximize the use of bandwidth and other network resources.
- Supports the tunneling of multiple Layer 3, non-IP protocols, and not just IP Layer 3 services, as is the case with Layer 3 solutions, such as Multiprotocol Label Switching (MPLS) VPNs.
- All DOCSIS services, including BPI+ encryption and authentication, continue to be supported for all cable modems.

How to Configure the Transparent LAN Service over Cable

This section contains the following:

Configuring IEEE 802.1Q VLAN Mapping

This section describes how to enable Layer 2 mapping on the Cisco CMTS, and then to map particular cable modems to an IEEE 802.1Q VLAN.

Enabling and Configuring Layer 2 Tunneling for IEEE 802.1Q Mapping

This section describes how to enable Layer 2 mapping on the Cisco CMTS, and then to map particular cable modems to IEEE 802.1Q VLANs on an Ethernet, Fast Ethernet, or Gigabit Ethernet interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2-vpn-service dot1q** or**cable l2-vpn-service xconnect nsi dot1q** **Example:** `Router(config)# cable l2-vpn-service dot1q` `or` **Example:** `Router(config)# cable l2-vpn-service xconnect nsi dot1q`	**Note** Use cable l2-vpn-service xconnect nsi dot1q command at this step, for Cisco IOS Release 12.2(33)SCC and later. Use cable l2-vpn-service dot1q command, for Cisco IOS Releases 12.2(33)SCA and 12.2(33)SCB. Enables Layer 2 tunneling for IEEE 802.1Q VLAN mapping. **Note** It is not required to configure VLAN trunking on the Cisco CMTS. Though VLAN trunking is supported, be aware of additional impact of VLAN trunking on the Cisco CMTS.
Step 4	**cable dot1q-vc-map** *mac-address ethernet-interface vlan-id* [*cust-name*] **Example:** `Router(config)# cable dot1q-vc-map 0000.0C04.0506 FastEthernet0/0 10`	Maps the specified MAC address of a cable modem to the indicated VLAN and Ethernet, Fast Ethernet, or Gigabit Ethernet interface. **Note** Repeat this command for each cable modem that is to be mapped to an IEEE 802.1Q VLAN.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Creating the IEEE 802.1Q VLAN Bridge Group

This section describes the minimum configuration needed to configure a Cisco router, which is acting as an IEEE 802.1Q VLAN bridge aggregator, so that it can terminate the VLANs being used with the Transparent LAN Service over Cable feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:**	Enters global configuration mode.
Step 3	**interface** [**Ethernet** | **FastEthernet** | **GigabitEthernet** | **TenGigabitEthernet**] *x/0* **Example:** `Router(config)# interface fastethernet 1/0` **Example:** `Router(config-if)#`	Enters interface configuration mode for the Ethernet interface that is in slot *x* .
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.85 255.255.255.0`	Configures the interface with the specified IP address and subnet mask.
Step 5	**interface** [**Ethernet** | **FastEthernet** | **GigabitEthernet** | **TenGigabitEthernet**] *x/0.y* **Example:** `Router(config)# interface fastethernet 1/0.10` **Example:** `Router(config-if)#`	Creates a subinterface on the Ethernet interface that is in slot *x* . The valid range for *y* is 1 to 4294967293, with no default. **Note** Note 1: To simplify network management, set the subinterface number to the same value as the VLAN ID that will use this subinterface (which in this case is 10). The valid range for the subinterface number is 1 to 4095. Note 2: The steps to create a subinterface is not essential for dot1q tagging of frames but it is recommended.
Step 6	**bridge group** *number* **Example:** `Router(config-if)# bridge group 20`	Configures this subinterface to belong to the specified bridge group. The valid range for number is 1 to 255, with no default. **Note** Repeat steps Step 5 through Step 7 for each subinterface to be created and bridged.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Transparent LAN Service over Cable

This section lists sample configurations for the Transparent LAN Service over Cable feature on a CMTS router and on a Cisco router acting as an ATM bridge aggregator:

Example: Configuring IEEE 802.1Q VLAN Mapping

The following partial configuration for a Cisco uBR7246VXR router shows a typical configuration that shows a number of cable modems being mapped to two different IEEE 802.1Q VLANs.

```
cable l2-vpn-service dot1q
! Customer 1
cable dot1q-vc-map 000C.0e03.69f9 GigabitEthernet 1/0 10 Customer1
cable dot1q-vc-map 0010.7bea.9c95 GigabitEthernet 1/0 11 Customer1
cable dot1q-vc-map 0010.7bed.81c2 GigabitEthernet 1/0 12 Customer1
cable dot1q-vc-map 0010.7bed.9b1a GigabitEthernet 1/0 13 Customer1
! Customer 2
cable dot1q-vc-map 0002.fdfa.137d GigabitEthernet 1/0 20 Customer2
cable dot1q-vc-map 0006.28f9.9d19 GigabitEthernet 1/0 21 Customer2
cable dot1q-vc-map 000C.7b6b.58c1 GigabitEthernet 1/0 22 Customer2
cable dot1q-vc-map 000C.7bed.9dbb GigabitEthernet 1/0 23 Customer2
cable dot1q-vc-map 000C.7b43.aa7f GigabitEthernet 1/0 24 Customer2
cable dot1q-vc-map 0050.7302.3d83 GigabitEthernet 1/0 25 Customer2
...
```

Example: Configuring IEEE 802.1Q Bridge Aggregator

The following example shows a router being used as a bridge aggregator to transmit VLANs across the same Fast Ethernet interface, using IEEE 802.1Q tagging.

```
!
interface GigabitEthernet0/1
 ip address 10.10.10.31 255.255.255.0
 duplex full
 speed auto
!
interface GigabitEthernet0/1.10
 description Customer1-site10
 encapsulation dot1Q 10
 bridge-group 200
interface GigabitEthernet0/1.11
 description Customer1-site11
 encapsulation dot1Q 11
 bridge-group 200
interface GigabitEthernet0/1.12
 description Customer1-site12
 encapsulation dot1Q 12
```

```
 bridge-group 200
interface GigabitEthernet0/1.13
 description Customer1-site13
 encapsulation dot1Q 13
 bridge-group 200
!-----------------------------------
interface GigabitEthernet0/1.20
 description Customer2-site20
 encapsulation dot1Q 20
 bridge-group 201
interface GigabitEthernet0/1.21
 description Customer2-site21
 encapsulation dot1Q 21
 bridge-group 201
interface GigabitEthernet0/1.22
 description Customer2-site22
 encapsulation dot1Q 22
 bridge-group 201
interface GigabitEthernet0/1.23
 description Customer2-site23
 encapsulation dot1Q 23
 bridge-group 201
interface GigabitEthernet0/1.24
 description Customer2-site24
 encapsulation dot1Q 24
 bridge-group 201
interface GigabitEthernet0/1.25
 description Customer2-site25
 encapsulation dot1Q 25
 bridge-group 201
!
bridge 200 protocol ieee
bridge 201 protocol ieee
...
```

Additional References

Related Documents

Related Topic	Document Title
ATM Interface Configuration	Configuring ATM in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/configuration/guide/fwan_c.html
ATM Interface Configuration	Configuring ATM in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/configuration/guide/fwan_c.html
ATM Interface Command Reference	ATM Commands in the *Cisco IOS Wide-Area NetworkingCommand Reference,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/command/reference/fwan_r.html

Related Topic	Document Title
Virtual LAN Configuration	Virtual LANS in the *Cisco IOS Switching Services Configuration Guide* , Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/fswtch_c.html
Virtual LAN Command Reference	*Cisco IOS Switching Services Command Reference* , Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

Standards

Standards	Title
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification
IEEE 802.1Q, 1998 Edition	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

RFCs

RFCs[70]	Title
RFC 1163	A Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
RFC 2233	DOCSIS OSSI Objects Support
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2665	DOCSIS Ethernet MIB Objects Support

RFCs[70]	Title
RFC 2669	Cable Device MIB

70 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

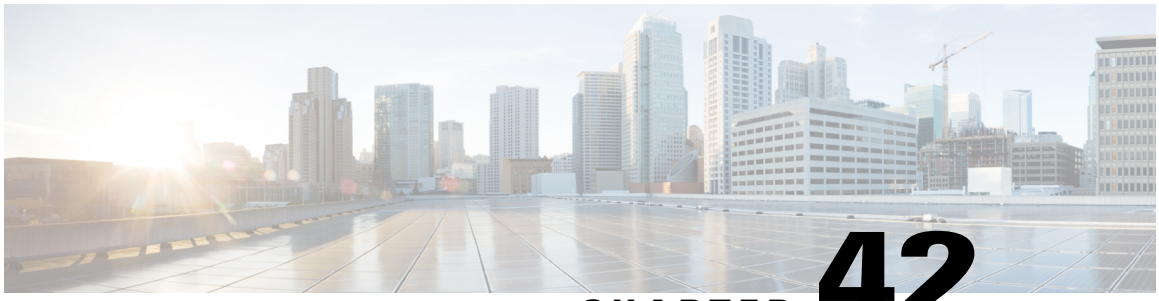
Feature Information for Transparent LAN Service over Cable

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 113: Feature Information for Transparent LAN Service over Cable

Feature Name	Releases	Feature Information
Transparent LAN Service over Cable	Release 12.2(11)BC3	This feature was introduced for Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers to support Layer 2 encapsulation over ATM networks. The following sections provide information about this feature: The following commands were introduced or modified: • **cable dot1q-vc-map** • **cable l2-vpn-service atm-vc** • **cable l2-vpn-service dot1q** • **cable vc-map** • **debug cable l2-vpn** • **show cable l2-vpn vc-map**
IEEE 802.1Q Virtual Local Area Network	Release 12.2(15)BC2	Support was added for IEEE 802.1Q Virtual Local Area Network (VLAN) tagging on the Cisco uBR7246VXR universal broadband router. Support was also added for identifying mappings with a customer name. The following commands were introduced or modified: • **show cable l2-vpn dot1q-vc-map**
Transparent LAN Services	Release 12.3(9a)BC	Support was added for Transparent LAN Services (TLS) for the following Cisco CMTS platforms: • IEEE 802.1Q on the Cisco uBR10012 router with Cisco uBR10012 PRE2 performance routing engine modules • ATM on the Cisco uBR7246VXR router



CHAPTER 42

VRF Steering for Cisco CMTS Routers

First Published: June 20, 2011

The virtual routing and forwarding (VRF) steering feature allows provisioning of data traffic from cable modems to be contained to a specified VRF instance. This enables all traffic from and to a particular set of cable modems to be constrained to a VRF instance.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for VRF Steering

The table shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 114: Cable Hardware Compatibility Matrix for VRF Steering

Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[71]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCF and later releases** • Cisco uBR-MC28U/X • Cisco uBR-MC88V
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCF and later releases** • Cisco uBR-MC28U/X • Cisco uBR-MC88V

71 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

Restrictions for VRF Steering

- Customer premise equipment (CPE) cannot specify a VRF instance unlike the cable modem.
- Only a single instance of the cable vrf-steering cable-modem command is supported.
- Only IPv4 is supported.

Information About VRF Steering

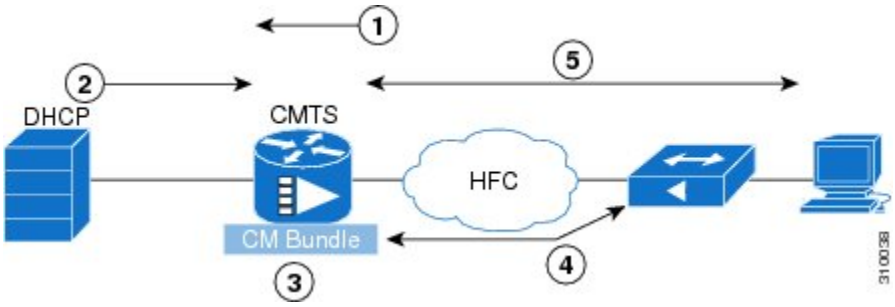
The VRF steering feature is developed to address the need for accommodating more IPv4 addresses when customers run out of IPv4 addresses for their CPE. This solution helps customers expand their existing IP address space until they move to the IPv6 address mode.

The availability of new IPv4 addresses is quickly coming to an end. In order to continue provisioning new subscribers, operators must switch to IPv6. This feature is designed to give the operators additional time to switch to IPv6 by expanding the use of non-traditional IPv4 addresses within their network. This feature allows the operator to create a private VRF for cable modems that are not routable outside of the operator network and choose any address since the CM addresses will not be routed externally. The CPE devices will continue to be provisioned with globally routable addresses, allowing them to peruse the internet.

VRF Steering Process

The figure and the following sequence of events describe the VRF steering process.

Figure 25: VRF Steering Process



1. The master bundle interface has at least 2 sub-bundles configured. The CPE is routed using the global sub-bundle interface. The CM is routed using the private VRF sub-bundle interface.
2. CM address negotiation happens using helper-address of the private VRF sub-bundle interface.
3. CPE address negotiation happens using helper-address of the global sub-bundle interface.
4. The Cisco CMTS steers all cable modem data traffic into the VRF. CM traffic that is punted to the route processor (RP) is forwarded only on the CM VRF.
5. At this point the CPE is able to get an IP address using the global Dynamic Host Configuration Protocol (DHCP) server. Since the CPE traffic is not classified, it uses the global routing table and is routable.

How to Configure VRF Steering

Configuring the VRF Steering

This section describes how to configure a VRF instance on the Cisco CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf vrf-name** **Example:** `Router(config)# ip vrf CM-VRF` **Example:** `rd 100:100` **Example:** `route-target export 100:100` **Example:** `route-target import 100:100`	Defines a VRF instance and enters the interface configuration mode. • vrf-name—Name assigned to a VRF.
Step 4	**ip access-list extended** access-list-name **Example:** `Router(config)# ip access-list extended vrfcpe` **Example:** `permit ip 111.1.0.0 0.0.255.255 any` **Example:** `permit ip 112.1.0.0 0.0.255.255 any` **Example:** `permit ip 101.1.0.0 0.0.255.255 any`	Specifies an extended IP access list to enable filtering for packets with IP helper-address destinations. • access-list-name—Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

	Command or Action	Purpose
Step 5	**route-map** map-tag **permit** sequence-number **Example:** `Router(config)# route-map cpe permit 10` **Example:** `Router(config)#route-map cpe permit 10` **Example:** `Router(config-route-map)# match ip address vrfcpe` **Example:** `Router(config-route-map)# set global`	Defines the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing. The route map needs to reference the ACL. • map-tag—A meaningful name for the route map. • sequence-number—Number that indicates the position a new route map will have in the list of route maps already configured with the same name.
Step 6	**interface bundle** *n* **Example:** `Router(config-if)# interface Bundle1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n*—Interface bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. The numeric identifiers may range from 1 to 255.
Step 7	**cable vrf-steering cable-modem** *vrf-name* **Example:** `Router(config-if)# cable vrf-steering cable-modem CM-VRF`	Steers or directs cable modems to the specified VRF in the cable interface configuration mode. • *vrf-name*—The VPN Routing/ Forwarding instance name.
Step 8	interface bundle n.1 **Example:** `Router(config-if)# interface Bundle1.1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n.1*—Interface sub-bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 9	**ip address ip-address mask secondary** **Example:** `Router(config-subif)# ip address 112.1.1.1 255.255.0.0 secondary`	Sets a secondary IP address for an interface. **Note** Create a primary interface address before setting a secondary IP address. If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.

	Command or Action	Purpose
Step 10	**cable dhcp-giaddr policy** **Example:** `Router(config-subif)# cable dhcp-giaddr policy`	(Optional) Selects the control policy, so that the primary address is used for cable modems and the secondary addresses are used for hosts and other CPE devices.
Step 11	cable helper-address *IP-address* **Example:** `Router(config-subif)# cable helper-address 72.10.10.2`	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast DHCP packets in cable subinterface configuration mode. • IP-address—The IP address of a DHCP server to which UDP broadcast packets will be sent.
Step 12	**exit** **Example:** `Router(config-subif)# exit`	Exits the subinterface configuration mode.
Step 13	interface bundle n.2 **Example:** `Router(config-if)# interface Bundle1.2`	Adds the selected interface to the virtual sub-bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n.2*—Interface sub-bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 14	ip vrf forwarding vrf-name **Example:** `Router(config-subif)# ip vrf forwarding CM-VRF`	Associates a VRF instance with an interface or subinterface. • vrf-name—Name assigned to a VRF.
Step 15	**ip address ip-address mask** **Example:** `Router(config-subif)# ip address 192.0.2.1 255.255.255.0`	Sets a primary or secondary IP address for the specified interface. • *mask*—Mask for the associated IP subnet address.
Step 16	**ip policy route-map** *map-tag* **Example:** `Router(config-subif)# ip policy route-map cpe`	Identifies a route map to use for policy routing on an interface. • *map-tag*—Name of the route map to use for policy routing. The name must match a map-tag value specified by a route-map command.
Step 17	**cable helper-address** IP-address **Example:** `Router(config-subif)# cable helper-address 192.0.2.200`	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast Dynamic Host Configuration Protocol (DHCP) packets in cable subinterface configuration mode. • IP-address—The IP address of a DHCP server to which UDP broadcast packets will be sent.

	Command or Action	Purpose
Step 18	**cable source-route** **Example:** `Router(config-subif)# cable source-route`	Configures the VRF source route in the cable modem's sub- bundle interface configuration mode. **Note** This command is applicable to Cisco uBR10012 routers only.
Step 19	**exit** **Example:** `Router(config-subif)# exit`	Exits the subinterface configuration mode.

Troubleshooting Tips

Run the debug cable bundle vrf-steering command to display the interfaces selected during the configuration.

Configuration Examples for VRF Steering

This section provides the following configuration examples:

Example: VRF Steering for CMTS Routers

The following example shows how to configure VRF steering on CMTS routers:

```
Router> enable configure terminal
ip vrf CM-VRF
rd 100:100
route-target export 100:100
route-target import 100:100
! These commands apply to all the devices attached on this cable bundle.
!
interface Bundle1
 no ip address
 no cable arp filter request-send
 no cable arp filter reply-accept
 cable vrf-steering cable-modem CM-VRF
end
!Subinterface for CPEs.
!
interface Bundle1.1
 ip address 112.1.1.1 255.255.0.0 secondary
 ip address 111.1.1.1 255.255.0.0 secondary
 ip address 101.1.1.1 255.255.0.0
 cable dhcp-giaddr policy
 cable helper-address 72.10.10.2
! Subinterface for CMs. These CMs go into CM-VRF
!
interface Bundle1.2
 ip vrf forwarding CM-VRF
 ip address 72.10.10.1 255.255.0.0
 ip policy route-map cpe
 cable helper-address 72.10.10.2
 cable source-route
end
```

```
! Create ACL for CPE
!
ip access-list extended vrfcpe
 permit ip 111.1.0.0 0.0.255.255 any
 permit ip 112.1.0.0 0.0.255.255 any
 permit ip 101.1.0.0 0.0.255.255 any
!
! Create route-map for CPE
!
route-map cpe permit 10
 match ip address vrfcpe
 set global
end.
```

Verifying VRF Steering

To verify or view which VRF contains a specific cable modem in the ARP cache table, use the show ip arp vrf command in privileged EXEC mode.

The following is sample output from the show ip arp vrf command:

```
Router # show ip arp vrf
CM-VRF
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  203.0.113.1               0   0018.742c.6e00  ARPA   FastEthernet0/0/0
Internet  203.0.113.2               -   0014.f1e4.fb58  ARPA   FastEthernet0/0/0
Internet  198.51.100.1              -   0014.f1e4.fc31  ARPA   Bundle1.2
Internet  198.51.100.2              0   001e.6bfb.34e8  ARPA   Bundle1.2
Internet  198.51.100.3              0   0007.0e07.9f1f  ARPA   Bundle1.2
Internet  198.51.100.5              0   0025.2eaf.6bea  ARPA   Bundle1.2
Internet  198.51.100.6              0   001a.c3ff.d1a4  ARPA   Bundle1.2
Internet  198.51.100.7              0   001e.6bfb.1c7e  ARPA   Bundle1.2
```

Additional References

The following sections provide references related to the VRF Steering feature.

Related Documents

Related Topic	Document Title
Cisco uBR10012 Universal Broadband Router Documentation	*IPv6 on Cable* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ cmts_ipv6.html *Virtual Interface Bundling for the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ cmts_cbl_if_bundlg.html *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/ installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/ configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/ prod_release_notes_list.html
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/ cbl_book.html

Standards

Standard	Title
None	

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
None	

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VRF Steering

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

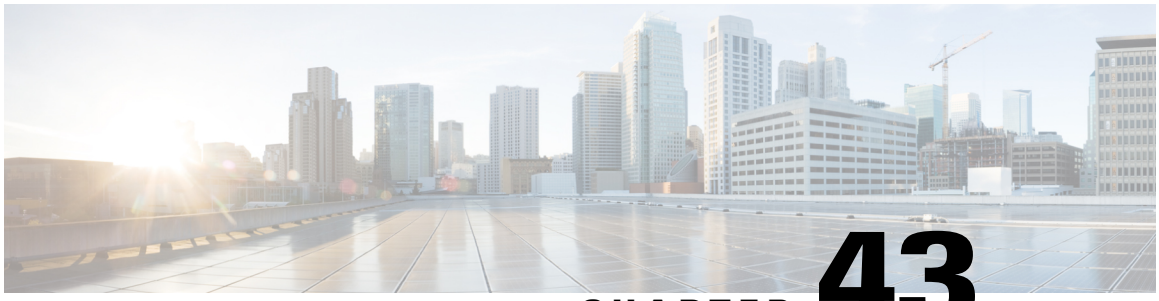
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 115: Feature Information for VRF Steering

Feature Name	Releases	Feature Information
VRF Steering	12.2(33)SCF	The VRF steering feature allows provisioning of data traffic from cable modems to be contained to a specified VRF instance. In Cisco IOS Release 12.2(33)SCF, this feature was introduced on the Cisco CMTS routers. The following commands were introduced or modified: • cable source-route • cable vrf-steering cable-modem • **ip vrf** • **show ip arp vrf**

PART VI

Layer 3 and Bundle Interface Features



CHAPTER 43

DOCSIS 3.0 Multicast Support on the CMTS Routers

First Published: December 18, 2008

Last Updated: May 27, 2013

Cisco IOS Release 12.2(33)SCB introduces multicast improvements based on Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 for the Cisco cable modem termination system (CMTS) routers. DOCSIS 3.0 multicast support improves bandwidth efficiency and allows service providers to offer differentiated quality of service for different types of traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the DOCSIS 3.0 Multicast Support

- DOCSIS 3.0-compliant Cisco CMTS and DOCSIS 3.0-enabled cable modems are required.
- Cisco CMTS must be MDF-enabled by default.
- Quality of service (QoS) parameters must be configured for various multicast sessions.
- Multicast Baseline Privacy Interface Plus (BPI+) profile must be configured before adding a Multicast BPI+ profile to a Multicast BPI+ multicast group.

Table below shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Table 116: DOCSIS 3.0 Multicast Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCC and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V[72] **Cisco IOS Release 12.2(33)SCE and later releases** • Cisco UBR-MC3GX60V[73]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[74]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V

72 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

73 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

74 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for the DOCSIS 3.0 Multicast Support

- You cannot disable explicit tracking.
- For multicast QoS, you must define three objects and templates, Service-Class, Group-QoS-Config (GQC), and Group-Config, and associate them to a particular bundle or forwarding interface.

- You must define a default service class and GQC before defining objects and templates.
- Multicast authorization is disabled by default and you should enable and configure it properly.
- Static multicast feature is always enabled and you cannot disable it.
- The service flow attribute-based selection will be ignored if the group configuration is configured on the default forwarding interface.
- A profile group cannot be deleted when it is applied to any forwarding or bundle interface. However, the same restriction does not apply to the global profile group. A global profile group can be deleted even when it is assigned to a forwarding or bundle interface.
- The multicast DSID feature is supported only on DOCSIS 3.0-compliant cable modems.
- The cable multicast mdf-disable wb-incapable-cm command disables multicast downstream service identifier (DSID) forwarding capability on the cable modem, which impacts the DSID capability between the Cisco CMTS and the cable modem.
- The multicast traffic to CPE increases two-fold after changing the multicast QoS configuration or the service-flow attribute during an active session. The traffic replication will continue till the default session timeout period (180 seconds). After the session timeout, the multicast DSID is removed from both Cisco CMTS and CM, and normal multicast traffic flow is resumed.
- For the DOCSIS 3.0 Multicast support feature to function properly, the CPE and the CM must be in the same virtual routing and forwarding (VRF) interface.

Information About the DOCSIS 3.0 Multicast Support

IP multicast, an integral technology in networked applications, is the transmission of the same information to multiple recipients. Any network application, including cable networks, can benefit from the bandwidth efficiency of multicast technology. Two new technologies—Channel Bonding and Single Source Multicast (SSM)—are expected to dramatically accelerate multicast deployment.

The channel bonding and SSM technologies dramatically increase the operational efficiency of the existing hybrid fiber-coaxial (HFC) network. Using the multicast improvements, the cable operators can seamlessly deliver advanced services like video on demand (VoD), internet protocol television (IPTV), and facilitate interactive video and audio, and data services.

The following sections explain the benefits of DOCSIS 3.0 Multicast Support:

Multicast DSID Forwarding

DOCSIS 3.0 multicast support introduces centralized control at the Cisco CMTS to provide flexibility and scalability to support a large array of multicast protocols. It replaces the Internet Group Management Protocol (IGMP), version 2 snooping infrastructure, which was part of the DOCSIS 1.1 and 2.0 models. Now, the Cisco CMTS allocates an unique Downstream Service Identifier (DSID) to identify every multicast stream. These DSIDs are sent to the CMs that use these DSIDs to filter and forward Multicast traffic to the CPEs.

The multicast DSID forwarding (MDF) provides the following benefits:

- Unique identification of packet stream across bonding group within a MAC domain.
- Designation of packet stream as either Any Source Multicast (ASM) or Source Specific Multicast (SSM) per multicast channel.

- Implementation of multicast DSID management on the Route Processor (RP) makes it operate on a standalone basis.
- Snooping of all upstream signal control packets by the Cisco CMTS to find the customer premises equipment (CPE) on the Multicast DSID-based Forwarding (MDF) enabled CM and allocates DSID from the pool.
- Transmission of allocated DSIDs to the CM through Dynamic Bonding Change (DBC) message.
- Reuse of DSIDs on other MDF-enabled CMs in the same bonding group, joining the multicast session.
- Removal of DSIDs from the CM through a DBC message by the Cisco CMTS after a multicast session leave event.
- Release of DSID to the pool by the Cisco CMTS when the last member leaves the bonding group.
- The following DSIDs are preallocated for each primary downstream (modular and integrated cable interfaces) to forward general query messages. These DSIDs form part of the multicast group signaling protocol. Other multicast groups, do no use these DSIDs.
    - IGMPv2 general query (IPv4)
    - IGMPv3 general query (IPv4)
    - MLDv1 general query (IPv6)
    - MLDv2 general query (IPv6)
    - Preregistration of DSID (IPv6)
- Allocation of DSID ensures traffic segregation between virtual private networks (VPNs) for DOCSIS 3.0 MDF-enabled CMs. For example, two clients from two VPNs joining the same multicast will get two distinct DSIDs.

Multicast Forwarding on Bonded CM

Multicast packets to the DOCSIS 3.0-enabled CMs are transmitted as bonded packets with DSID extension header on the primary bonding group if the Secondary Multicast Bonding Group is disabled. Multicast packets for MDF-disabled or pre-DOCSIS 3.0 CMs are transmitted as non-bonded without DSID extension header. For more information on this feature, refer to Multicast Secondary Bonding Group, on page 1122.

In a network, where only MDF-enabled or MDF-disabled CMs exist, the traffic is segregated using field types. The MDF-enabled CM forwards the frame with the field type and the MDF-disabled CM drops it. The DSID labeling ensures that MDF-enabled CM gets a copy of the multicast session to prevent “cross talk”.

For hybrid CMs (MDF-enabled and MDF-disabled CMs) that do not support field type forwarding, you should configure per session encryption or security association identifier (SAID) isolation to ensure traffic segregation. DOCSIS 3.0 mandates that if the hybrid CM fails to forward field type frames, the Cisco CMTS should employ multicast security association identifier (MSAID) isolation. This isolation is achieved by assigning different MSAID to each replication, one to bonded CM and another to the non-bonded or hybrid CM. This helps to prevent CMs from receiving duplicate traffic.

Static TLV Forwarding

As per DOCSIS 3.0 specifications, the Cisco CMTS must support Static Multicast. When the CM tries to register with the Cisco CMTS, the Cisco CMTS checks whether Static Multicast Encoding is present in the

CM configuration file. If the Static Multicast Encoding is present, the Cisco CMTS sends a DSID corresponding to each Static Multicast channel in the Registration-Response (REG-RSP) message.

The Multicast DSID management is located at RP and the cable line card (CLC) has to contact the RP for proper DSID assignment. The CLC also caches the response from RP to eliminate the need to communicate to the RP for subsequent Static Multicast encoding. Refer BPI+ Support, on page 1119 for more details on SAID assignment for Static Multicast functionality.

IPv6 Multicast

The Cisco CMTS routers support both IPv4 and IPv6 protocol stacks. The basic multicast character of IPv6 is similar to that of IPv4 multicast. Multicast in IPv6 can be either a Multicast Listener Discovery (MLD), version 1 that supports ASM or MLDv2 that supports SSM. DOCSIS 3.0 specifications demand support for both MLDv1 and MLDv2.

The MLD component uses the protocol descriptor block (PDB) for the multicast. The PDB contains all information about the session, including source, group, and number of sources. IPv6 mandates that all information, such as source MAC and Cisco CMTS service identifier (SID), should be accessed from the PDB. The packet header in IPv6 contains the correct forwarding interface and DSID information. When the packet arrives at the Cisco CMTS, it is identified as an IPv6 packet and sent to the correct bundle.

For more details on IPv6, refer to the IPv6 on Cable document available at the following location: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_ipv6.html

Explicit Tracking

The Cisco CMTS can perform explicit tracking with IGMPv3 support. The IGMPv3 removes the report suppression feature associated with the IGMPv2 specification enabling the Cisco CMTS to get the complete information on session and host information. This benefits the IGMP Fast Leave processing and DSID management for each CM.

A host or session database is used to track hosts (IP/MAC) joining a particular multicast session. From the host, you can track the CM based on the SID and cable downstream interface. This database also helps to determine whether the Cisco CMTS should remove the DSID from a particular CM when the multicast session is over.

BPI+ Support

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

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

Dynamic Multicast Encryption

The Cisco CMTS encrypts downstream multicast traffic to the CMs with a security association (SA), which is previously signaled to the CM. The security association identifier is defined per session and communicated

in a SA encoding through the MAC management message sent to the CM. The Cisco CMTS uses dynamic SA mechanism for DSID multicast forwarding in MDF-disabled CMs.

During a dynamic multicast join event, through IGMP or Multicast Listener Discovery (MLD), the Cisco CMTS checks the configuration table to see whether the session must be encrypted. If it requires encryption, the Cisco CMTS creates a multicast security association identifier (MSAID) and includes it in SA encoding with an add action in the Dynamic Bonding Change Request (DBC-REQ).

Static Multicast Encryption

During a static multicast encoding of Registration Request (REG-REQ), Cisco CMTS checks the configuration table at the RP through the Inter-Process Communication (IPC) to ascertain the need for encryption. If it requires encryption, the Cisco CMTS creates an MSAID and includes it in the SA encoding with an add action in the REG-RSP. The cable line card (CLC) can also cache the MSAID mapping for subsequent requests.

Multicast Join Authorization

DOCSIS 3.0 introduces the IP Multicast Join Authorization feature to control the IP multicast sessions joined by the IP multicast clients. The set of IP multicast clients reached through the CM includes the CM IP host stack itself. This feature controls only the joining of downstream IP multicast sessions and not the ability of any client to transmit IP multicast traffic upstream.

General guidelines for multicast join authorization are as follows:

- Cisco CMTS should authorize the IP multicast sessions joined by the IP multicast clients.
- IPv6 solicited node multicast sessions should be routed to IPv6 addresses through the Source Address Verification (SAV) feature.
- IP multicast sessions identified by static IP multicast encoding should be in the registration request of the CM.
- IPv6 or IPv4 multicast sessions which map to Layer 2 Ethernet multicast MAC address should be identified using the static multicast MAC address encoding in the registration request of the CM.
- For an IP multicast session, the CM should have a “permit” action for the highest priority matching rule “IP Multicast Join Authorization Session.”
- When the management object “Default IP Multicast Join Authorization Action” is set to “permit”, the IP multicast session should not match any “IP Multicast Join Authorization” rule.

With the above guidelines, static MAC multicast and static IP multicast are authorized by default. The Cisco CMTS enforces IP multicast join authorization by signaling or not signaling multicast DSIDs and /or SAs. For a pre-DOCSIS 3.0 CM, multicast BPI+ must be used.

The cable multicast auth enable default-action command is used to enable or disable Multicast Join Authorization feature.

Multicast Session Limits

DOCSIS 3.0 supports per CM multicast session where you can configure Multicast Session Encoding in the CM configuration file as specified in the DOCSIS 3.0 specifications.

The Cisco CMTS receives the encoding of REG-REQ from the CLC and the CLC would notify the Route Processor through Inter-Process Communication about CM registration.

The Cisco CMTS supports a session limit between 0 and 65535 per CM. If the CM does not include encoding, the Cisco CMTS uses the default Maximum Multicast Sessions. The multicast session limit only enforces the dynamic join session and does not restrict Static Multicast sessions.

IP Multicast Profile

In an IP multicast profile, the Cisco CMTS provides the capability to store 16 profiles, each with 256 session rules. Each session rule consists of the Source prefix, Group prefix, Priority, and “Permit” or “Deny” action. The rule priority is used to determine the best matching rule.

The CM can store up to 16 IP multicast profiles and the Cisco CMTS makes use of them to configure a multicast profile for the CM. If the CM does not have any IP multicast profile defined, the Cisco CMTS uses the Default IP multicast profile name. If the IP multicast profile defined in the CM configuration file is not available in the Cisco CMTS, an empty multicast profile with the same name is created by the Cisco CMTS, which can be configured later by the operator.

If the join request of a CM to a multicast session does not match any of the session rules, the Cisco CMTS uses the default IP multicast join authorization action, which can be either “Permit” or “Deny.” When the session rules are changed, the Cisco CMTS reapplies the latest rules on all subsequent join requests.

Default Multicast Authorization Profiles

Cisco IOS Release 12.2(33)SCC introduces the option to create default multicast authorization profiles. These profiles are used to register modems without an authorization profile in their configuration file. Like other profiles, the default profile group can store up to 16 default multicast authorization profiles. The default profile group also maintains a sorted list of session rules from all default profiles, based on priority. Each configured default profile can store up to 256 session rules.

The session rules are used to authorize modems without a profile name in their configuration file. When an IGMP join for a group is received from such a modem, it is matched against the rules in the default profile group. If the rules match, the join action is permitted, else the globally configured default action is taken.

When a session rule is created, the Cisco CMTS assigns an ID to that rule. These session rule IDs are assigned sequentially and are unique per profile. If there are 5 session rules in a profile, they are assigned IDs ranging from 0 to 4. If a session rule is deleted, the next rule in the profile is assigned with that ID. For example, when a session rule with ID 3 is deleted, the next rule in the profile will be assigned ID 3.

The DOCSIS 3.0 operations support system (OSS) specification mandates that the session rules have to be identified within a profile using an identifier value that has a range of 1 to 4,294,967,295 (32 bit).

The **cable multicast auth profile-name** command is used to define a cable multicast authorization profile and to set it as the default profile.

MDF-Disabled CM

To enforce multicast authorization in MDF-disabled and pre-DOCSIS 3.0 CMs, the Cisco CMTS should configure per-session encryption based on Security Association-Multicast Authorization Profile (SA-MAP) authorization. The Cisco CMTS should check the SA-MAP request against the multicast authorization profile of the CM to verify if it is an authorized flow and reply with a SAID accordingly.

Multicast Quality of Service Enhancement

DOCSIS 3.0 mandates that the CMTS should not admit any flow exceeding the session limit. Though the current Multicast QoS (MQoS) session limit admits the session, it fails to provide any QoS for sessions exceeding the session limit.

Note Multicast packets are sent using the default Group Service Flows (GSF) when the Multicast QoS feature is disabled.

As part of DOCSIS 3.0 requirements for Multicast QoS, Cisco IOS Release 12.2(33)SCC provides support for Group Classifier Rules (GCR). The Cisco CMTS determines the set of Group Configurations (GCs) whose session range matches the multicast group address. For SSM, the source address is also used to identify the matching GCs. A GCR is created for each matching GC and linked to the multicast session. The GCR is assigned also with an unique identifier, SAID, and Group Service Flow (GSF).

The following conditions are used to select the GC entries:

- The GC entry with the highest rule priority is selected, if more than one GC entry matches.
- All matching GC entries are selected, when multiple GCs have the same highest rule priority.

The GCR classification is done based on type of service (TOS) fields. The TOS specifier in the GCR is used to choose the correct GCR when multiple GCRs match a single multicast session.

Note When two multicast group configurations (GCs) have the same session range and configuration (under global or bundle configuration), then the same forwarding interface selection is not guaranteed.

Non-IP multicasts and broadcast packets use GSF. They are similar to individual service flows and are shared by all the CMs on a particular Digital Command Signal (DCS) matching the same GCR. A single GSF is used for multicast sessions matching different GCs using the same aggregate GQC.

The legacy multicast QoS **cable match address** command is replaced from Cisco IOS Release 12.2(33)SCB onwards to allow multiple system operators (MSOs) to move to the new multicast QoS model. The old command is automatically translated to the new command during system bootup while parsing the startup configuration. After system configuration, the old command is disabled from the parser chain.

For details on DOCSIS QoS support, refer to the DOCSIS QoS Support section of the DOCSIS WFQ Scheduler on the Cisco CMTS Routers guide.

Multicast Secondary Bonding Group

The DOCSIS 3.0-compliant CM can receive multicast packets from non-primary (or bonded) channels using the MDF support at the CMTS.

The multicast secondary bonding group is defined as a shared bonding group or RF channel that feeds more than one fiber node through an optical split. This allows CMs from different primary bonding groups and channels to listen to one or more shared sets. The multicast packets are replicated only to the shared downstream channel set, which helps conserve the downstream bandwidth.

DOCSIS 3.0 defines attribute-based service flow creation, which allows the Cisco CMTS to make more “intelligent” decisions on the selection of bonding group or individual channel for unicast and multicast forwarding.

The Multicast Secondary Bonding Group provides the following benefits:

- New MQoS and attribute-based forwarding for Multicast Secondary Bonding Group.
- The primary downstream interface acts as a forwarding interface for narrowband CMs.
- The following algorithm is used to select a forwarding interface for wideband CMs:
  - A primary bonding group is selected if a group-config matching the session is present in it. MQoS parameters are taken from the group-config.
  - A primary bonding group is selected if a group-config is not present at the bundle level or at the global level.
  - A group-config found at the bundle level or global level is used to find the Group-QoS-Config (GQC) and eventually the attribute and forbidden bit-masks, which are then used to find the interface.
  - All Wideband Cable Modems (WCMs) in a bundle use the same secondary bonding group if a bundle-level group-config or global-level group-config is configured.
- The IGMP report ignores a source if the given source address fails to find a matching interface.
  - If a matching interface is found, that interface is used for forwarding and the MQoS parameters are taken from the matching group-config from the forwarding interface or bundle interface or global level.
  - If a matching interface is not found, then the IGMP report is ignored.
- For a static join, attribute-based forwarding is not supported, and only the primary downstream is used.

Multicast Replication Session Cache

Cisco IOS Release 12.2(33)SCH introduces the multicast replication session cache feature to improve CPU utilization on the Cisco uBR10012 router. In Cisco IOS releases before Cisco IOS Release 12.2(33)SCH, the Cisco uBR10012 router supported multicast replication session creation and deletion, and IGMP leave and join operations of existing multicast replication sessions. By caching the existing multicast replication sessions and reusing them when an IGMP join is received and matched, the CPU performance of the Cisco uBR10012 router improves.

This feature is supported for dynamic IPv4 group join operations on single type multicast sessions. When a new IGMP join is received, the session cache is searched for an existing replication session. If a match is found, the session is reused.

Note The multicast replication session cache is *not* supported for IPv6 multicast sessions and aggregate multicast sessions.

The multicast replication session cache can be configured globally for all the interfaces on the Cisco uBR10012 router or can be configured at the interface level for the forwarding interface. The cache size value can be configured using the **cable multicast ses-cache** command.

The **clear cable multicast cache ses-cache** command clears the multicast cache counters on the forwarding interface as well as the cached entry. The **show cable multicast ses-cache** command displays the multicast replication session information, both at the global level and the interface level.

The multicast replication cache session is enabled only on the active RP and not on the standby RP.

Load Balancing

The Load Balancing feature modified in Cisco IOS Release 12.2(33)SCB will not load balance a CM while a multicast stream is going on for that particular CM. It utilizes the Explicit Tracking Database, which holds complete information on the CM subscription to achieve this. For more information on Load Balancing, refer to the Configuring Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers document.

Bonded DS Admission Control

Multiple MAC domains may share a single DS bonding group. Similarly, CPEs from multiple MAC domains could listen to a Wideband multicast service flow. The devices could join or leave the multicast group in any order.

The bonded multicast service flows are admitted and created on the Guardian line card rather than on a specific host line card.

The admission control for Wideband DS interfaces should also take into account the multicast service flow bandwidth usage. The entire DS bonding group bandwidth is available for every single MAC domain and the multicast traffic for committed information rate (CIR) reservations is based on the current CIR bandwidth usage of the sharing MAC domains.

The aggregate use of CIR bandwidth is limited by the bonding group definition. However, a single MAC domain could reserve the entire bandwidth if other MAC domains are not using it for CIR purposes.

The following criteria is used for DS bonding group bandwidth distribution:

- The Guardian line card can use 50 percent of the available bandwidth for multicast. The rest of the bandwidth is equally distributed to other MAC domain hosts sharing the bonding group.
- If any of the MAC domain or Guardian line card exceeds 90 percent of the bandwidth reservation of the entire bonding group, the remaining bandwidth is given to the same MAC domain or Guardian line card to effectively utilize the small unusable fragments.

When the number of MAC domains sharing the DS bonding group increases, the available bandwidth decreases proportionally. It also limits the service flow CIR that can be admitted on the Guardian line card or MAC domain host.

Based on the example given in Table below, three MAC domain hosts are sharing a DS bonded interface with 60 Mbps bandwidth. Initially, the Guardian line card is getting 30 Mbps and the other MAC domain hosts are getting 10 Mbps each. If the multicast usage goes up by 30 Mbps, the available bandwidth will be 60 – 30 = 30 Mbps. This new bandwidth will be shared between the Guardian line card and MAC domain hosts. Now, the Guardian line card would get 15 Mbps and the MAC domains would get 5 Mbps each. This limits the highest CIR service flow that can be admitted to MAC domain hosts to 5 Mbps, although the available bandwidth is still 30 Mbps. If any of the MAC domain hosts keeps admitting service flows much smaller (for example, 100 Kbps) compared to 5 Mbps, it could reserve close to 30 Mbps provided the service flow admission is spaced apart by 3 seconds.

Table 117: Sharing a DS Bonded Interface Between Guardian Line Card and Three MAC Domains

WB Interface Bandwidth		Guardian Bandwidth		MAC Domain Host 1 Bandwidth		MAC Domain Host 2 Bandwidth		MAC Domain Host 3 Bandwidth	
Available	Reserved	Available	Reserved	Available	Reserved	Available	Reserved	Available	Reserved
60	0	30	0	10	0	10	0	10	0
30	30	15	30	5	0	5	0	5	0
0.6	59.4	0.3	30	0.1	29.4	0.1	0	0.1	0

Multicast DSID Forwarding Disabled Mode

For any application that needs the cable modem to perform IGMP snooping, the MDF on the cable modem must be disabled. Cable modems registered in MDF-enabled mode by the Cisco CMTS do not perform IGMP snooping because MDF forwarding is based on DSID filtering. In Cisco IOS Release 12.2(33)SCD3, the **cable multicast mdf-disable** command is introduced in global configuration mode to disable the MDF capability on the cable modem.

This command is configured on the route processor and is downloaded to the cable line card via the configuration update. The configuration does not change the Cisco CMTS forwarding mechanism or DSID allocation. The Cisco CMTS allocates the DSID and the multicast packet is encapsulated with the DSID header. This does not affect traffic forwarding on the MDF-disabled cable modem. According to DOCSIS3.0 specification, pre-DOCSIS2.0 or MDF-disabled cable modems ignore the DSID header and continue multicast forwarding based on the Group Media Access Control (GMAC) from IGMP snooping. When the cable modem runs in MDF-disabled mode, only IGMPv2 is supported and the Cisco CMTS drops IGMPv3 and MLD messages.

Multicast encryption based on BPI+ is not supported on non-MDF cable modems, if IGMP SSM mapping is used. A non-MDF cable modem is either a pre-DOCSIS 3.0 cable modem or a DOCSIS 3.0 cable modem running in MDF-disabled mode.

MDF1 Support for DOCSIS 2.0 Hybrid Cable Modems

Starting with Cisco IOS Release 12.2(33)SCE4, the Cisco CMTS router enables MDF capability for DOCSIS 2.0 hybrid cable modems, IPv6, and other cable modems that advertise MDF capability to allow IPv6 packet forwarding. In earlier releases, MDF capability was disabled for wideband incapable cable modems and cable modems that were not DOCSIS 3.0-compliant. The **wb-incapable-cm** keyword was added to the cable multicast mdf-disable command to disable MDF on all DOCSIS 2.0 hybrid cable modems including DOCSIS Set-Top Gateway (DSG) hybrid embedded cable modems to support IGMP snooping.

DSG Disablement for Hybrid STBs

In Cisco IOS Release 12.2(33)SCE4 and later, the **cable multicast mdf-disable** command with the wb-incapable-cm keyword prevents all DOCSIS 2.0 DSG embedded cable modems from receiving DSG multicast traffic besides disabling MDF support. In Cisco IOS Release 12.2(33)SCF2, the wb-incapable-cm keyword was modified to supersede the restriction on DSG multicast traffic.

In Cisco IOS Release 12.2(33)SCF2 and later, the wb-incapable-cm keyword disables MDF capability only on non-DSG DOCSIS 2.0 hybrid cable modems. To disable MDF capability on all DSG embedded cable modems (DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid), a new keyword, DSG, was introduced in Cisco IOS Release 12.2(33)SCF2.

Note After disabling MDF capability, you must run **clear cable modem reset** command to bring all DSG embedded cable modems online.

Table below provides details of the cable multicast mdf-disable command behavior in Cisco IOS Release 12.2(33)SCF2 and later.

Table 118: cable multicast mdf-disable Command Behavior in Cisco IOS Release 12.2(33)SCF2

Command	Behavior
cable multicast mdf-disable	Disables MDF capability of all cable modems connected to the Cisco CMTS router.
cable multicast mdf-disable wb-incapable-cm	Disables MDF capability of all non-DSG DOCSIS 2.0 hybrid cable modems.
cable multicast mdf-disable dsg	Disables MDF capability of all DSG embedded cable modems, including DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid modems.

Benefits of MDF1 Support

- Supports IPv6 on different known cable modem firmware types.
- Disables the MDF capability on the Cisco CMTS.
- Supports In-Service Software Upgrade (ISSU) and line card high availability.

How to Configure the DOCSIS 3.0 Multicast Support

This section describes the following tasks that are required to implement DOCSIS 3.0 Multicast Support on Cisco CMTS Routers:

Configuring Basic Multicast Forwarding

To configure a basic multicast forwarding profile that can be applied to a DOCSIS 3.0 multicast configuration, use the **ip multicast-routing** command. You must configure a multicast routing profile before you can proceed with a multicast group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**IP multicast-routing** [**vrf**] **Example:** `Router(config)# IP multicast-routing vrf`	Enables multicast routing globally or on a particular virtual routing and forwarding (VRF) interface. • *vrf* —(Optional) Specifies the name of the VRF instance.
Step 4	**interface bundle** *number* **Example:** `Router(config)# interface bundle 1`	Configures the interface bundle and enters interface configuration mode. • *number*—Bundle interface number. The valid range is from 1 to 255.
Step 5	**IP pim sparse-mode** **Example:** `Router(config-if)# IP pim sparse-mode`	Configures sparse mode of operation. **Note** In Cisco IOS Release 12.2(33)SCA and later releases, a Cisco CMTS router must have a Protocol Independent Multicast (PIM) rendezvous point (RP) configured for the PIM sparse mode. The RP is configured using the ip pim rp-address command or Auto-RP configuration protocol.
Step 6	**IP pim sparse-dense-mode** **Example:** `Router(config-if)# IP pim sparse-dense-mode`	Configures the interface for either sparse mode or dense mode of operation, depending on the mode in which the multicast group is operating.
Step 7	**IP igmp version version-number** **Example:** `Router(config-if)# IP igmp version 3`	Configures the interface to use IGMP version 3. • *version-number* —IGMP version number used on the router.

Configuring Multicast DSID Forwarding

The multicast DSID forwarding is enabled by default. You cannot configure this feature.

Configuring Explicit Tracking

The Explicit Tracking feature is enabled by default. You cannot configure it.

Configuring Multicast QoS

To configure a Multicast QoS profile that can be applied to a DOCSIS 3.0 configuration, use the **cable multicast group-qos** command. You must configure a Multicast QoS profile before you can add a Multicast QoS profile to a QoS multicast group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service class** *class-index* **name** *service-class-name* **Example:** `Router(config)# cable service class 1 name MQOS_DEFAULT`	Configures the name of the cable service class. • *class-index* —Class ID for the class to be modified. Valid range is from 1 to 255. • *service-class-name*—Service class name.
Step 4	**cable service class** *class-index* **downstream** **Example:** `Router(config)# cable service class 1 downstream`	Configures the downstream for the cable service class.
Step 5	**cable service class** *class-index* **max-rate** *maximum-bandwidth-allowed* **Example:** `Router(config)# cable service class 1 max-rate 10000000`	Configures the maximum allowed bandwidth for the cable service class.
Step 6	**cable service class** *class-index* **min-rate** *cir* **Example:** `Router(config)# cable service class 1 min-rate 1000000`	Configures the minimum committed information rate for the cable service class.

	Command or Action	Purpose
Step 7	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn MQOS_DEFAULT aggregate`	Specifies the default service class name for the QoS profile. • *default*—Specifies the default QoS profile number for the cable multicast QoS group. • *service class name*—Service class name for the QoS profile.
Step 8	**cable multicast qos group** *number* **priority** *value* **Example:** `Router(config)# cable multicast qos group 20 priority 1`	Configures a multicast QoS group and enters multicast QoS configuration mode, and specifies the priority of the cable multicast QoS group. • *number*—QoS profile number for the cable multicast QoS group. The valid range is from 1 to 255. • *value*—Cable multicast QoS group priority. The valid range is from 1 to 255.
Step 9	**application-id** *app-id* **Example:** `Router(config-mqos)# application-id 10`	Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group. The valid range is from 1 to 65535.
Step 10	**session-range ip-address ip-mask** **Example:** `Router(config-mqos)# session-range 230.0.0.0 255.0.0.0`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 11	**tos** *tos-value-low tos-value-high tos-mask* **Example:** `Router(config-mqos)# tos 1 6 15`	Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for a multicast QoS group. The valid range for each is from 0 to 255. • *tos-value-low*—MQoS Group ToS low value. • *tos-value-high*—MQoS Group ToS high value. • *tos-mask*—MQoS Group ToS mask value.
Step 12	**cable multicast qos group** *number priority value* [**global**] **Example:** `Router(config)#cable multicast qos group 20 priority 63 global`	Specifies the multicast QoS group identifier. • *number*—Cable multicast QoS group number. The valid range is from 1 to 255. • *priority value*—Specifies the priority of the cable multicast QoS group. The valid range is from 1 to 255. • **global**—(Optional) Specifies that the multicast QoS group configuration is applied to all cable interfaces.

Configuring a Multicast BPI+ Support

To configure a multicast BPI+ profile that can be applied to a QoS group configuration, use the **cable multicast qos group** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number* **algorithm** {**128bit-aes** | **40bit-des** | **56bit-des**} **Example:** `Router(config)# cable multicast group-encryption 30 algorithm 56bit-des`	Configures a group encryption profile. • *number*—Number of a specific cable multicast QoS group encryption profile. The valid range is from 1 to 255. • **algorithm**—Specifies that the data encryption standard (DES) as either 128, 56 or 40 bits.
Step 4	**cable multicast qos group** *gc-id* priority value [global] **Example:** `Router(config)# cable multicast qos group 20 priority 63 global`	Configures a multicast QoS group and enters multicast QoS configuration mode. • *gc-id* —Cable multicast QoS group number. The valid range is from 1 to 255. • *priority value*—Specifies the priority of the cable multicast QoS group. The valid range is from 1 to 255. • *global* —(Optional) Specifies that the multicast QoS group configuration is applied to all cable interfaces.
Step 5	**session-range ip-address ip-mask** **Example:** `Router(config-mqos)# session-range 230.0.0.0 255.0.0.0`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 6	**group-encryption** *group-encrypt-id* **Example:** `Router(config-mqos)# group-encryption 30`	Specifies a group encryption number.

Configuring a Multicast Join Authorization

To configure a multicast join authorization to control the IP multicast sessions joined by the IP multicast clients, use the **cable multicast authorization** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast auth enable default-action** { *permit* | *deny* } **max-sessions** *limit* **Example:** `Router(config)# cable multicast auth enable default-action deny max-sessions 10`	Enables multicast authorization and sets the maximum sessions limit. • *permit* —Enables multicast authorization by default. • *deny* —Denies multicast authorization by default. • *limit* —Maximum number of dynamic multicast sessions allowed per CM. Maximum value allowed is 65535.
Step 4	**cable multicast auth profile-name** *profile-name* [**default**] **Example:** `Router(config-mauth)# cable multicast auth profile-name GOLD default`	Configures the multicast authorization profile, and (optionally) sets it as the default profile. • *profile-name* —Name of the authorization profile to be used. • *default* —Specifies that the profile name should be treated as the default profile.
Step 5	**match rule** { *ipv4* | *ipv6* } *source-prefix group-prefix priority-value* {*permit* | *deny* } **Example:** `Router(config-mauth)# match rule ipv4 source 0.0.0.0/0 230.0.0.0/16 128 permit`	Configures the match rule, rule priority, and its related action. • *ipv4*—Matching IPv4 group address or prefix length (for example, 224.1.1.1/16). • *ipv6*—Matching IPv6 group address or prefix length (for example, FEDC:BA98:7654:3210::/<prefix-length>). • *source-prefix* —Matching source address prefix. • *group-prefix* —Matching group address prefix. • *priority-value* —Cable multicast authorization profile priority. • *permit* —Specifies whether to allow specified packets to be forwarded. • *deny* —Specifies whether to allow specified packets to be rejected.

	Command or Action	Purpose

Selecting a Forwarding Interface Based on Service Flow Attribute

The Service Flow Attribute feature allows a bonded CM to listen to multiple bonding groups, and using the interface-specific bit-masks, the CM can select the best route to receive multicast traffic.

Service Flow Attribute

The Service Flow Attribute feature allows selection of a forwarding interface based on the DOCSIS 3.0 construct named "service flow attribute mask." Every interface has an attribute bit-mask depicting attributes of that interface. The multicast service class specified in the group QoS configuration contains required and forbidden attribute bit-masks. If a bonded CM can listen to multiple bonding groups (wideband interfaces), using specific bit-masks in the service class as well as on the bonding group, then one of these bonding groups can be selected for forwarding of multicast traffic.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service class** *class-index* **Example:** `Router(config)# cable service class 10`	Configures the service class name. • *class-index* —Class index. Valid range is from 1 to 255.
Step 4	**cable service class** *class-index* **downstream** **Example:** `Router(config)# cable service class 10 downstream`	Configures the downstream for the selected service class. • *downstream* —Specifies the downstream for the service class.
Step 5	**cable service class** *class-index* **max-rate** *maximum-rate* **Example:** `Router(config)# cable service class 10 max-rate 1000000`	Configures the maximum rate for the selected service class. • *max-rate* —Configures the maximum rate for the service class.

	Command or Action	Purpose
		• *maximum-rate* —Maximum reserved rate. Valid range is from 0 to 4,294,967,295.
Step 6	**cable service class** *class-index* **min-rate** *minimum-rate* **Example:** `Router(config)# cable service class 10 min-rate 100000`	Configures the minimum rate for the selected service class. • *min-rate* —Configures the minimum rate for the service class. • *minimum-rate* —Minimum reserved rate. Valid range is from 0 to 4,294,967,295.
Step 7	**cable service class** *class-index* **req-attr-mask** *required-attribute-mask* **Example:** `Router(config)# cable service class 10 req-attr-mask 8000000F`	Configures the required attribute mask for the selected service class. • *req-attr-mask* —Configures the required attribute mask for the service class. • *required-attribute-mask* —Required attribute mask value. Valid range is from 0 to FFFFFFFF.
Step 8	**cable service class** *class-index* **forb-attr-mask** *forbidden-attribute-mask* **Example:** `Router(config)# cable service class 10 forb-attr-mask 7FFFFF0`	Configures the forbidden attribute mask for the selected service class name. • *forb-attr-mask* — Configures the forbidden attribute mask for the service class. • *forbidden-attribute-mask* —Forbidden attribute mask value. Valid range is from 0 to FFFFFFFF.
Step 9	**cable multicast group-qos** *number* **scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos 1 scn 10 mcast10 aggregate`	Configures the cable multicast group QoS identifier, service class name, and multicast value. • *number* —Cable multicast QoS group profile number. Valid range is from 1 to 255. • *scn* —Configures a service class name. • *service-class-name* —Service class name. • *aggregate* —Specifies aggregate service flow for sessions in the same MQoS group.
Step 10	**cable multicast qos group** *group* **priority** *priority* **Example:** `Router(config)# cable multicast qos group 1 priority 1`	Configures the cable MQoS group configuration on the bundle interface. • *group* —Cable MQoS group number. Valid range is from 1 to 255. • *priority priority* —Specifies the cable MQoS group priority.

	Command or Action	Purpose
Step 11	**session-range** *session-range mask* **group-qos** *qos* **Example:** `Router(config-mqos)# session-range 230.1.1.1 255.255.255.255 group-qos 1`	Enters MQoS configuration mode and specifies session range and group QoS. • *session-range session-range* —Configures the MQoS group session range. • *mask* —Session range group prefix mask. • *group-qos* —Specifies the MQoS group QoS identifier. • *qos* —MQoS group QoS number. Valid range is from 1 to 255.
Step 12	**interface bundle** *number* **ip address** *ip mask* **ip pim sparse-mode ip helper-address** *helper-address* **cable multicast qos group** *group* **Example:** `Router(config)# interface Bundle1` `ip address 40.1.1.1 255.255.255.0` `ip pim sparse-mode` `ip helper-address 2.39.16.1` `cable multicast-qos group 1`	Configures the interface bundle with the IP address, helper address, and MQoS group. • *number* —Bundle interface number. Valid range is from 1 to 255. • *ip address* —Specifies the IP address range and mask. • *ip* —IP address range. • *mask* —IP address subnet mask. • *ip pim sparse-mode* —Enables PIM sparse mode operation. • *ip helper-addressv* —Specifies a destination address for UDP broadcasts. • *helper-address* —Destination IP address.
Step 13	**interface wideband-cable {slot/port |** *slot*/*subslot*/*bay*:*port-number}* **description cable rf-channel** *rf-channel* **bandwidth-percent** *percent-value* **cable bundle** *number* **cable bonding-group-id** *id-num* **cable rf-channel** *rf-port* **bandwidth-percent** *percent-value* **cable downstream attribute-mask attribute-***mask* **Example:** `Router(config)# interface Wideband-Cable1/0/0:0` **Example:** `description cable rf-channel 0 bandwidth-percent 40` **Example:** `cable bundle 1`	Selects the interface for forwarding based on the bit-masks specified in the service class and on the wideband interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ slot—3 to 6 ◦ port—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ slot—1 and 2 ◦ port—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are: ◦ slot—Wideband SPA interface processor (SIP) slot. Valid values are 1 to 3. ◦ subslot—Wideband SIP subslot. Valid value is 0.

	Command or Action	Purpose
	Example: `cable bonding-group-id 1` **Example:** `cable rf-channel 0 bandwidth-percent 10` **Example:** `cable rf-channel 1 bandwidth-percent 10` **Example:** `cable rf-channel 2 bandwidth-percent 10` **Example:** `cable downstream attribute-mask 8000FF00`	◦ bay—Wideband SIP bay where the wideband shared port adapter (SPA) is located. Valid values are 0 (upper bay) and 1 (lower bay). • *rf-channel*—Specifies RF channel associated with the wideband interface. • *rf-channel*—RF channel number. • *bandwidth-percent*—Specifies the percentage of bandwidth from this RF channel that is reserved for the wideband interface. • *percent-value*—Bandwidth percentage value. • *cable bundle*—Specifies the bundle number for bundling of cable interfaces. • *number*—Cable bundle number. • *cable bonding-group-id*—Specifies the cable interface bonding group. • *id-num*—Cable bonding group identifier. • *cable downstream attribute-mask*—Specifies the attribute mask for the downstream channel. • *attribute-mask*—Cable downstream interface attribute mask.
Step 14	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*bay*:*port-number*} **cable bundle** *number* **cable bonding-group-id** *id-num* **secondary** **Example:** **cable rf-channel** *rf-port* **bandwidth-percent** *percent-value* **cable downstream attribute-mask [attribute-***mask***]** **Example:** `Router(config)# interface wideband-cable1/0/0:1` `cable bundle 1` `cable bonding-group-id 2 secondary` `cable rf-channel 0 bandwidth-percent 40` `cable downstream attribute-mask 8000FFF0`	Selects the required attributes from the service class that match the interface attribute bit-mask.

	Command or Action	Purpose
Step 15	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*bay*:*port-number*} **cable bundle** *number* **cable bonding-group-id** *id-num* **secondary** **Example:** **cable** **rf-channel** *rf-port* **bandwidth-percent** *percent-value* **cable rf-channel** *rf-channel* **bandwidth-percent** *percent-value* **cable downstream attribute-mask** [*mask*] **Example:** `Router(config)# interface wideband-cable1/0/0:2` `cable bundle 1` `cable bonding-group-id 3 secondary` `cable rf-channel 1 bandwidth-percent 40` `cable rf-channel 2 bandwidth-percent 40` `cable downstream attribute-mask 8000000F`	Selects the required attributes from the service class that match the interface attribute bit-mask; and the forbidden attributes that do not match.

Configuring Multicast DSID Forwarding Disabled Mode

To disable MDF on the cable modem, use the **cable multicast mdf-disable** command in global configuration mode.

Note Multicast encryption based on BPI+ is not supported on non-MDF cable modems, if IGMP SSM mapping is used.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast mdf-disable [wb-incapable-cm]** **Example:** `Router(config)# cable multicast mdf-disable`	Disables MDF capability on the cable modem. • wb-incapable-cm—(Optional) Turns off the MDF capability on the wideband incapable cable modems.
Step 4	exit **Example:** `Router(config)# exit` `Router#`	Exits the global configuration mode.

Configuring Multicast Replication Session Cache at the Forwarding Interface

This section describes the multicast replication session cache configuration for a wideband interface on the Cisco uBR10012 router.

To configure multicast replication session cache at the interface level on the Cisco uBR10012 router, first configure a forwarding interface: modular, integrated or wideband.

Note The multicast replication cache can be configured globally for all interfaces on the Cisco uBR10012 router using the **cable multicast ses-cache** command**.**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** *slot*/*subslot*/*port*:*wideband-channel*	Enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS

	Command or Action	Purpose
	Example: `Router(config)# interface wideband-cable 6/0/1:22`	software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where a SPA interface processor (SIP) or a line card resides. • *subslot*—Secondary slot for a shared port adapter (SPA) or a line card. • *bay*—Bay in a SIP where a SPA is located. • *port*—Downstream port number. • *wideband-channel*—Wideband channel number.
Step 4	**cable multicast ses-cache***value* **Example:** `Router(config-if)# cable multicast ses-cache 100`	Configures the multicast replication session cache on wideband cable interface. • *value*—Multicast replication session cache size limit. The valid range is from 0 to 500. The default value is 0.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

How to Monitor the DOCSIS 3.0 Multicast Support

To monitor the DOCSIS 3.0 Multicast Support feature, use the following procedures:

Verifying the Basic Multicast Forwarding

To verify the configuration parameters for basic multicast forwarding, use the **show ip mroute** command as shown in the following example:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 230.1.1.1), 00:00:03/00:02:55, RP 30.1.1.1, flags: S
```

```
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:00:03/00:02:55, H
(*, 224.0.1.40), 00:12:02/00:02:19, RP 30.1.1.1, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:12:02/00:02:19
```

Note During parallel express forwarding (PXF) reload, all the dynamic multicast route (mroute) entries in the IP multicast routing table are deleted. Only the IGMP static group entries are retained. After the PXF reload, dynamic mroutes are populated in the IP multicast routing table only when next IGMP join is received.

To verify the multicast information for the specified virtual interface bundle, based on IGMPv3, use the **show cable bundle multicast** command as shown in the following example:

```
Router# show cable bundle 1 multicast

CableBundle Interface Source IP  Multicast IP    MAC Address
1    Bundle1.1 *       230.1.1.1    0100.5e00.0001
```

To verify the MAC forwarding table for the specified virtual interface bundle, based on IGMPv3, use the **show cable bundle forwarding** command as shown in the following example:

```
Router# show cable bundle 1 forwarding

MAC address Interface Flags Location link sublink
00c0.5e01.0203 Cable8/0/0 3 64E5BF60 0 64E5BE00
00c0.5e01.0203 Cable7/0/0 3 64E5BE00 0 0
00c0.5e01.0101 Cable8/0/0 3 64E5BEE0 0 64E5BE40
```

To verify the multicast routing table in the PXF processor for a specified group, use the **show pxf cpu mroute** command as shown in the following example:

Note The show pxf cpu command is supported only on Cisco uBR10012 universal broadband routers.

```
Router# show pxf cpu mroute 0.0.0.0

Shadow G/SG[5624]: s: 0.0.0.0 g: 224.0.1.40 uses: 0 bytes 0 flags: [D ] LNJ
Interface vcci offset rw_index mac_header
In : 0 0x000004
Shadow G/SG[3195]: s: 0.0.0.0 g: 234.5.6.7 uses: 0 bytes 0 flags: [5 ] NJ
Interface vcci offset rw_index mac_header
In : 0 0x000008
Out: Cable5/1/0 5 0x00002C 1B 00000026800001005E05060700010
Out: Cable6/1/1 9 0x000028 1A 00000026800001005E05060700010
Out: Cable6/0/0 6 0x000024 19 00000026800001005E05060700010
Out: Cable5/0/0 3 0x000020 18 00000026800001005E05060700010
Out: Cable7/0/0 A 0x00001C 17 00000026800001005E05060700010
Out: Cable7/1/1 C 0x000018 16 00000026800001005E05060700010
Out: Cable7/1/0 B 0x000014 15 00000026800001005E05060700010
Out: Cable6/1/0 8 0x000010 14 00000026800001005E05060700010
Out: Cable6/0/1 7 0x00000C 13 00000026800001005E05060700010
Out: Cable5/0/1 4 0x000008 12 00000026800001005E05060700010
```

To verify the multicast routes (mroutes) in the PXF processor for a specified group, use the **show pxf cable multicast** command as shown in the following example:

```
Router# show pxf cable multicast 0.0.0.0

MDB Flags: L - Local, F - Register flag, T - SPT-bit set, J - Join SPT
           Z - Multicast Tunnel, N- No FastSwitching
OIF Flags: P - Prune Flag, A - Assert Flag
PXF multicast switching for vrf default is enabled.
Mdb at index= 3 hash= 0xE9F7:
```

```
next_mdb_idx: 0, fib_root: 0x0001, source_addr: 0.0.0.0, group_addr: 230.1.1.1
uses: 0, bytes: 0, vcci_in: 0, oif: 0x000002
rpf_failed: 0, drop_others: 0
rp_bit_mask:0x00,  flags: [0xA0]
Ref Count=0, MDB Flags=0x0082, MDB FastFlags=0x10
```

Verifying the Multicast DSID Forwarding

To verify the entire DSID database content, use the **show cable multicast dsid** command as shown in the following example:

```
Router# show cable multicast dsid
Multicast Group    : 230.1.2.3
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
         StatIndex : 2           SAID: DEFAULT
Multicast Group    : 230.1.2.3
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
         StatIndex : 3           SAID: 8196
Multicast Group    : 230.1.2.3
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
StatIndex : 4 SAID: 8197
```

To verify the entire database content, use the **show cable multicast db** command as shown in the following example:

Router# **show cable multicast db**

```
interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc Sub Intfc Host Intfc CM Mac Hosts
Wi1/1/0:0 Bundle1 Ca5/0/0 0018.6852.8056 1
```

To verify the information for the registered and unregistered CMs, use the **show cable modem verbose** command as shown in the following example:

Router# **show cable modem 0010.7bb3.fcd1 verbose**

```
MAC Address : 00C0.7bb3.fcd1
IP Address : 10.20.113.2
Prim Sid : 1
QoS Profile Index : 6
Interface : C5/0/U5
sysDescr : Vendor ABC DOCSIS 2.0 Cable Modem
Upstream Power : 0 dBmV (SNR = 33.25 dBmV)
Downstream Power : 0 dBmV (SNR = ----- dBmV)
Timing Offset : 1624
Initial Timing Offset : 2812
Received Power : 0.25
MAC Version : DOC1.0
Qos Provisioned Mode : DOC1.0
Enable DOCSIS2.0 Mode : Y
Phy Operating Mode : atdma
Capabilities : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs : 0(Max CPEs = 1)
CFG Max-CPE : 1
Flaps : 373(Jun 1 13:11:01)
Errors : 0 CRCs, 0 HCSes
Stn Mtn Failures : 0 aborts, 3 exhausted
Total US Flows : 1(1 active)
Total DS Flows : 1(1 active)
```

```
Total US Data : 1452082 packets, 171344434 bytes
Total US Throughput : 0 bits/sec, 0 packets/sec
Total DS Data : 1452073 packets, 171343858 bytes
Total DS Throughput : 0 bits/sec, 0 packets/sec
Active Classifiers : 0 (Max = NO LIMIT)
DSA/DSX messages : reject all
Dynamic Secret : A3D1028F36EBD54FDCC2F74719664D3F
Spoof attempt : Dynamic secret check failed
Total Time Online : 16:16
```

Verifying the Explicit Tracking Feature

To verify explicit tracking information, use the **show cable multicast db** command as shown in the following example:

Router# **show cable multicast db**

```
Interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc  Sub Intfc  Host Intfc   CM Mac           Hosts
Mo1/1/0:0  Bundle1    Ca5/0/0      0018.6852.8056       1
```

Verifying the Multicast QoS Feature

To verify the cable MQoS details, use the **show cable multicast qos** commands as shown in the following example:

```
Router# show cable multicast qos ?
group-config Display Multicast Group Config information
group-encryption Display Multicast Group Encryption information
group-qos Display Multicast Group QOS information
Router# show cable multicast qos group-config
Multicast Group Config 1 : Priority 1
Group QOS - 1
Group Encryption - 1
Session Range - Group Prefix 230.0.0.0 Mask 255.0.0.0 Source Prefix 0.0.0.0 Mask 0.0.0.0
Router# show cable multicast qos group-encryption
Multicast Group Encryption 1 : Algorithm 56bit-des
Router# show cable multicast qos group-qos
Group QOS Index Service Class Control Igmp Limit Override
DEFAULT MQOS_DEFAULT Aggregate NO-LIMIT 1 MQOS Aggregate NO-LIMIT
```

To verify the DOCSIS service flows on a given cable interface, use the **show interface service-flow** command as shown in the following example:

```
Router# show interface cable 6/0 service-flow

Sfid  Sid   Mac Address     QoS Param Index Type    Dir    Curr   Active
BG/CH
                             Prov  Adm  Act                 State  Time
4     8193  ffff.ffff.ffff   3     3    3   sec(S)  DS     act    21h57m
5     8196  ffff.ffff.ffff   4     4    4   sec(S)  DS     act    00:17
```

To verify the parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command as shown in the following example:

Note The show pxf cpu command is supported only on Cisco uBR10012 universal broadband routers.

```
Router# show pxf cpu queue

FP queue statistics for Cable5/0/0
FP queue statistics for Cable6/0/0
Queue algorithm 0x0
```

```
Queue number 0 Shared
wq_avg_qlen 0 wq_flags_pd_offset 18A0001
wq_drop_factor 40
wq_buffer_drop 0 wq_limit_drop 0
wq_invalid_enq_wqb_drop 0 wq_invalid_deq_wqb_drop 0
wq_rnd_pkt_drop 0 wq_rnd_byte_drop 0
wq_static_qlen_drop 0
wq_len 0
Packet xmit 56414 Byte xmit 14322357
Queue number 15 Shared High priority
wq_avg_qlen 0 wq_flags_pd_offset 18A8001
wq_drop_factor 1000
wq_buffer_drop 0 wq_limit_drop 0
wq_invalid_enq_wqb_drop 0 wq_invalid_deq_wqb_drop 0
wq_rnd_pkt_drop 0 wq_rnd_byte_drop 0
wq_static_qlen_drop 0
wq_len 0
Packet xmit 0 Byte xmit 0
```

Verifying the Multicast BPI+ Support Feature

To verify information about the multicast sessions on a specific virtual forwarding interface, use the **show interface multicast-sessions** command as shown in the following example:

Router# **show interface wideband-Cable 5/1/2:0 multicast-sessions**

```
Default Multicast Service Flow 9 on Wideband-Cable5/1/2:0
Multicast Group    : 230.1.2.3
         Source    : N/A
         Act GCRs  : 2
         Interface : Bu123                 State: A      GI: Wi5/1/2:0   RC: 0
         GCR       : GC   SAID    SFID    Key   GQC    GEn
                     2    8244    14      27    2      1
                     1    8245    15      28    1      1
Aggregate Multicast Sessions on Wideband-Cable5/1/2:0
Multicast Group    : 230.1.2.3
         Source    : N/A
         GCRs      : 2
         Interface : Bu123                 State: A      GI: Wi5/1/2:0   RC: 0
         GCR       : GC   SAID    SFID    Key   GQC    GEn
                     2    8244    14      27    2      1
                     1    8245    15      28    1      1
```

To verify the service identifier (SID) information of the multicast sessions on a specific virtual forwarding interface, use the **show interface cable sid** command as shown in the following example:

Router# **show interface cable 5/1/0:0 sid 1**

```
Wideband SPA: 1/0    total index assigned: 0      multicast: 0
Wideband SPA: 1/1    total index assigned: 1      multicast: 1
SID : 8197      Latest : 2      Current : 1
  Wideband SPA:  WB channel : 0     blaze_index: 1
  Status[0] : 1  DES Key[0] : 1C7619321C8F0D73   DES IV[0]  :
166D1A291375011A
  Key Life[0]: 43171 sec
  Status[1] : 1  DES Key[1] : E5B0B2C23EA07B6    DES IV[1]  :
209E105D13E91F73
  Key Life[1]: 21571 sec
  Req : 0        Rply : 0        Rej : 0 Inv : 0 RxErr : 0
```

Verifying the Multicast Join Authorization

To verify the multicast profile information, use the **show cable modem auth-profile** command as shown in the following example:

```
Router# show cable modem 0019.474a.d518 auth-profile
Multicast Profile Information for  0019.474a.d518  IP: 20.1.2.3
Multicast Profile Group #           : 0
This CM's Session Limit             : 5
Profile Id          Profile
   0                goldservice
   1                platinumservice
   2                silverservice
```

To verify the multicast profile group, use the **show cable** multicast authorization profile-group command as shown in the following example:

```
Router# show cable multicast authorization profile-group 0
   ProfileGroup:  0,    CMs using this group: 4
   ProfileId   CMs        Profile
   ------------------------------
     0         4         goldservice
     1         4         platinumservice
     2         4         silverservice
   Auth Rule List for prof_group_index: 0
           Src                   Grp            Priority     Action
   ---------------------------------------------------------------------
           0.0.0.0/0            230.1.1.1/24        255       permit
```

To verify multicast profile list, use the **show cable** multicast authorization profile-list command as shown in the following example:

```
Router# show cable multicast authorization profile-list 0
       CMTS Authorization Profile List
       -------------------------------
   Profile Name: goldservice at index: 0
   Number of CMs using this Profile: 4
           Src                   Grp            Priority     Action
   ---------------------------------------------------------------------
           0.0.0.0/0            230.1.1.1/24        255       permit
```

Verifying the Service Flow Attributes

To verify the configuration of service flow attributes on the service class configuration, use the show cable service-class verbose command as shown in the following example:

```
Router# show cable service-class 10 verbose
Index:                                  10
Name:                                   mcast10
Direction:                              Downstream
Traffic Priority:                       0
Maximum Sustained Rate:                 1000000 bits/sec
Max Burst:                              3044 bytes
Minimum Reserved Rate:                  1000000 bits/sec
Minimum Packet Size                     0 bytes
Admitted QoS Timeout                    200 seconds
Active QoS Timeout                      0 seconds
Required Attribute Mask                 8000000F
Forbidden Attribute Mask                7FFFFFF0
Scheduling Type:                        Undefined
Max Latency:                            0 usecs
Parameter Presence Bitfield:            {0x3148, 0x0}
```

To verify the configuration of SF attributes on the Wideband interface configuration, use the **show running-config interface** command as shown in the following example:

```
Router# show running-config interface Wideband-Cable 1/0/0:2
interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3
 cable rf-channel 3
 cable downstream attribute-mask 8000000F
end
```

Verifying the Multicast Group Classifiers

To verify the details of the Group Classifier Rule, use the **show interface wideband-cable multicast-gcr** command as shown in the following example:

```
Router# show interface wideband-cable 1/1/0:0 multicast-gcr
Group Classifier Rules on Wideband-Cable1/1/0:0:
Classifier_id  Group_id  Group_Qos_id  Sid   SFID   ref_count
7              1         1             8196  10     1
8              2         1             8197  11     1
```

Troubleshooting Tips

Make sure that CM can listen to the RF-frequencies specified for the Wideband interfaced chosen for forwarding multicast traffic.

Verifying Multicast Replication Session Cache

To verify the cable multicast replication session cache information at the wideband interface, use the **show cable multicast ses-cache** command with the interface keyword as shown in the following example:

```
Router# show cable multicast ses-cache interface wi7/1/0:1
Fwd Intfc          Sub Intfc             Session (S,G)
Wi7/1/0:1          Bundle1              (30.30.30.30,226.0.0.20)
                   Bundle1              (30.30.30.30,226.0.0.22)
                   Bundle1              (30.30.30.30,226.0.0.23)
                   Bundle1              (30.30.30.30,226.0.0.21)
```

To verify the cable multicast replication session cache information at the modular-cable interface, use the **show cable multicast ses-cache** command with the interface keyword as shown in the following example:

```
Router# show cable multicast ses-cache int Mo6/0/1:0
Fwd Intfc           Sub Intfc             Session (S, G)
Mo6/0/1:0           Bundle1               (*, 230.0.8.138)
```

To verify the cable multicast replication session cache information at the global level, use the **show cable multicast ses-cache** command with the global keyword as shown in the following example:

```
Router# show cable multicast ses-cache global

Fwd Intfc          Sub Intfc             Session (S,G)
Wi7/1/0:0          Bundle1              (30.30.30.30,227.0.0.20)
                   Bundle1              (30.30.30.30,227.0.0.22)

Wi7/1/0:1          Bundle1              (30.30.30.30,226.0.0.20)
                   Bundle1              (30.30.30.30,226.0.0.22)
                   Bundle1              (30.30.30.30,226.0.0.23)
                   Bundle1              (30.30.30.30,226.0.0.21)
Mo6/0/1:0          Bundle1               (*, 230.0.8.138)
```

Configuration Examples for DOCSIS 3.0 Multicast Support

This section provides the following configuration examples:

Example: Configuring Basic Multicast Forwarding

Note The commands given below are required to enable the Cisco CMTS to forward multicast packets. However, Multicast QoS, BPI+, and Authorization features are all optional for multicast packets to be forwarded correctly.

In the following example, a basic multicast forwarding profile is configured.

```
ip multicast-routing
int g1/0/0
  ip pim sparse-dense-mode
int Bundle 1
  ip pim sparse-mode
  ip igmp version 3
```

Example: Configuring Multicast QoS

Note A default service class and GQC must be defined before proceeding with configuring Multicast QoS.

In the following example, Multicast QoS is configured. You should define three objects and templates and then associate these to a particular bundle or forwarding interface. The objects are Service-Class, Group-QoS-Config (GQC), and Group-Config.

```
cable service class 1 name MQOS_DEFAULT
cable service class 1 downstream
cable service class 1 max-rate 10000000
cable service class 1 min-rate 1000000
cable multicast group-qos default scn MQOS_DEFAULT aggregate
cable multicast group-qos 10 scn MQOS single
cable multicast qos group 20 priority 1
application-id 10
session-range 230.0.0.0 255.0.0.0
tos 1 6 15
vrf name1
cable multicast qos group 20 priority 63 global
```

Example: Configuring Multicast BPI+

In the following example, Multicast BPI+ is configured. The Multicast BPI+ basically reuses the Multicast QoS CLI model under Group-Config object.

```
cable multicast group-encryption 30 algorithm 56bit-des
cable multicast qos group 40 priority 2 global
  session-range 230.0.0.0 255.0.0.0
  group-encryption 30
interface Cable5/0/0
  cable multicast-qos group 40
```

Example: Configuring Multicast Join Authorization

In the following example, multicast join authorization is configured:

```
cable multicast auth enable default-action  deny  max-sessions 10
cable multicast auth profile GOLD
   match rule ipv4 source 0.0.0.0/0 230.0.0.0/16 128 permit
   match rule ipv4 source 10.1.1.1/8 232.0.0.0/8 128 permit
end
```

Example: Configuring Forwarding Interface Selection Based on Service Flow Attribute

In the following example, the service flow attribute-based Forwarding Interface Selection is configured. To send multicast traffic for group 230.1.1.1, interface W1/0/0:2 is selected. The multicast QoS parameters are taken from group qos 1 (effectively from service class “mcast10”).

```
cable service class 10 name mcast10
cable service class 10 downstream
cable service class 10 max-rate 1000000
cable service class 10 min-rate 1000000
cable service class 10 req-attr-mask 8000000F
cable service class 10 forb-attr-mask 7FFFFFF0
cable multicast group-qos 1 scn mcast10 aggregate
cable multicast qos group 1 priority 1
session-range 230.1.1.1 255.255.255.255
 group-qos 1
interface Bundle1
 ip address 40.1.1.1 255.255.255.0
 ip pim sparse-mode
 ip helper-address 2.39.16.1
 cable multicast-qos group 1
end
interface Wideband-Cable1/0/0:0
 description cable rf-channel 0 bandwidth-percent 40
 cable bundle 1
 cable bonding-group-id 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable downstream attribute-mask 8000FF00
interface Wideband-Cable1/0/0:1
 cable bundle 1
 cable bonding-group-id 2 secondary
 cable rf-channel 0 bandwidth-percent 40
 cable rf-channel 1 bandwidth-percent 40
 cable downstream attribute-mask 8000FFF0
interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3 secondary
 cable rf-channel 1 bandwidth-percent 40
 cable rf-channel 2 bandwidth-percent 40
 cable downstream attribute-mask 8000000F
```

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cisco uBR7200 series universal broadband routers, the Cisco uBR10012 universal broadband routers, and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Additional References

The following sections provide references related to the DOCSIS 3.0 Multicast Support on the CMTS Routers.

Related Documents

Related Topic	Document Title
CMTS cable commands	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.htmlCisco IOS CMTS Cable Command Reference
Multicast VPN and DOCSIS 3.0 Multicast QoS	Multicast VPN and DOCSIS 3.0 Multicast QoS Support
DOCSIS 3.0 QoS Support	DOCSIS WFQ Scheduler on the Cisco CMTS Routers

Standards

Standard	Title
CM-SP-CMCIv3-I01-080320	Cable Modem to Customer Premise Equipment Interface Specification
CM-SP-MULPIv3.0-I08-080522	MAC and Upper Layer Protocols Interface Specification
CM-SP-OSSIv3.0-I07-080522	Operations Support System Interface Specification
CM-SP-PHYv3.0-I07-080522	Physical Layer Specification
CM-SP-SECv3.0-I08-080522	Security Specification

MIBs

MIB[75]	MIBs Link
• DOCS-MCAST-AUTH-MIB • DOCS-MCAST-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

75 Not all supported MIBs are listed.

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DOCSIS 3.0 Multicast Support on the CMTS Routers

Table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note Table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 119: Feature Information for DOCSIS 3.0 Multicast Support on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Multicast DSID Forwarding	12.2(33)SCB	The Multicast DSID Forwarding makes use of the DSID to identify the CMs intended to join the Cisco CMTS for the multicast session. It filters and forwards the multicast packets from the CM to the Cisco CMTS. The following sections provide information about this feature: Multicast DSID Forwarding, on page 1117 Configuring Basic Multicast Forwarding, on page 1126 Configuring Multicast DSID Forwarding, on page 1127 The following command was introduced or modified: • **show cable multicast dsid**
Multicast Forwarding on Bonded CM	12.2(33)SCB	Multicast packets are sent to the CM on the primary bonding group it has registered, if Secondary Multicast Bonding Group feature is disabled. The following sections provide information about this feature: Multicast Forwarding on Bonded CM, on page 1118 The following command was introduced or modified: • **show cable modem verbose**

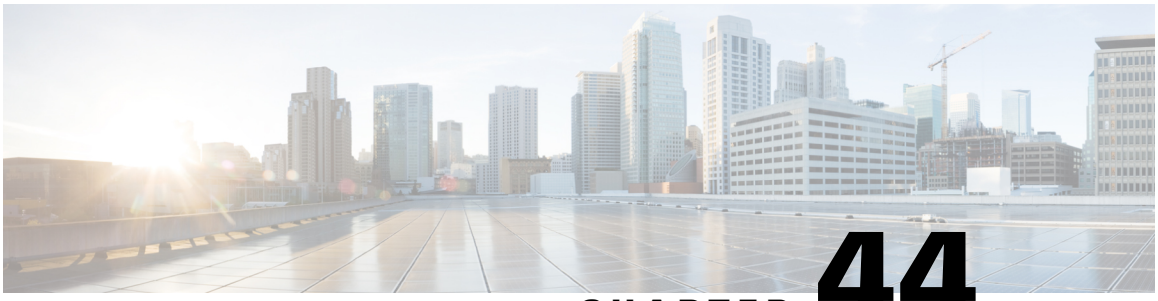
Feature Name	Releases	Feature Information
Explicit Tracking	12.2(33)SCB	IGMPv3 support removes report suppression enabling the Cisco CMTS to get the complete session and host information. The following sections provide information about this feature: Explicit Tracking, on page 1119 Configuring Multicast QoS, on page 1128 The following command was introduced or modified: • **show cable multicast db**
BPI+ Support	12.2(33)SCB	The BPI feature provides data privacy across the HFC network by encrypting traffic flows between the router and the cable operator's CMTS. The BPI+ (BPI Plus) feature provides more secure authentication of cable modems through the use of digital certificates. The following sections provide information about this feature: BPI+ Support, on page 1119 Configuring a Multicast BPI+ Support, on page 1130 Configuring a Multicast Join Authorization, on page 1131

Feature Name	Releases	Feature Information
Multicast Join Authorization	12.2(33)SCB	The Multicast Join Authorization feature allows control of the IP multicast sessions joined by the IP multicast clients. The following sections provide information about this feature: Multicast Join Authorization, on page 1120 Configuring a Multicast Join Authorization, on page 1131 The following commands were introduced or modified: • **cable multicast authorization** • **cable multicast authorization profile** • **match rule**
Multicast Quality of Service Enhancement	12.2(33)SCB	DOCSIS 3.0 mandates that the CMTS should not admit any flow exceeding the session limit. The current Multicast QoS session limit admits the session, however, it fails to provide any QoS for sessions exceeding the session limit. The following sections provide information about this feature: Multicast Secondary Bonding Group, on page 1122 The following command was introduced or modified: • **cable multicast group-qos**

Feature Name	Releases	Feature Information
Multicast Secondary Bonding Group	12.2(33)SCB	The Multicast Secondary Bonding Group is defined as a shared bonding group or RF channel that feeds more than one fiber node through an optical split. This allows CMs from different primary bonding groups and channels to listen to one or more shared sets. The following sections provide information about this feature: Multicast Secondary Bonding Group, on page 1122
Default Multicast Authorization Profile	12.2(33)SCC	The Default Multicast Authorization Profile feature allows to create default multicast authorization profile group to authorize modems without a profile name in their configuration file. The following sections provide information about this feature: Default Multicast Authorization Profiles, on page 1121 The following command was introduced or modified: • **cable multicast auth profile-name**
Group Classifier Rules	12.2(33)SCC	Group Classifier Rules allows the Cisco CMTS to determine the set of GC entries whose session range matches the new SSM session. The following sections provide information about this feature: Multicast Quality of Service Enhancement, on page 1122 Verifying the Multicast Group Classifiers, on page 1144 The following command was introduced or modified: • **show interface multicast-gcr**

Feature Name	Releases	Feature Information
DOCSIS 3.0 Multicast	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following commands were introduced or modified: • **show cable multicast dsid** • **show cable modem auth-profile**
Multicast DSID Forwarding Disabled Mode	12.2(33)SCD3	A global CLI is introduced to disable MDF on the cable modem. The following sections provide information about this feature: Multicast DSID Forwarding Disabled Mode, on page 1125 Configuring Multicast DSID Forwarding Disabled Mode, on page 1136 The following command was introduced or modified: • **cable multicast mdf-disable**
MDF1 Support for DOCSIS 2.0 Hybrid Cable Modems	12.2(33)SCE4	The Cisco CMTS router enables the MDF capability in a DOCSIS 2.0 hybrid CM to allow IPv6 packet forwarding. The following sections provide information about this feature: • Multicast DSID Forwarding Disabled Mode, on page 1125 • Configuring Multicast DSID Forwarding Disabled Mode, on page 1136 The following command was modified: • **cable multicast mdf-disable**

Feature Name	Releases	Feature Information
DSG Disablement for Hybrid STBs	12.2(33)SCF2	In Cisco IOS Release 12.2(33)SCF2 and later, MDF capability can be disabled on all DSG embedded cable modems using the **cable multicast mdf-disable** command with the DSG keyword. For details about this functionality, see the DSG Disablement for Hybrid STBs, on page 1125. The **cable multicast mdf-disable** command was modified to support this feature.
Multicast replication session cache	12.2(33)SCH	The following sections provide information about this feature: • Multicast Replication Session Cache, on page 1123 • Configuring Multicast Replication Session Cache at the Forwarding Interface, on page 1137 The following commands were introduced or modified: • **cable multicast ses-cache** • **clear cable multicast ses-cache** • **show cable multicast ses-cache** {**global** | **interface**}[**summary** | **verbose**]



CHAPTER 44

IPv6 on Cable

First Published: February 18, 2008

Last Updated: January 28, 2016

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Support for the IPv6 on Cable feature is introduced in Cisco IOS Release 12.2(33)SCA for the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers to extend IP addressing functionality on these Cisco cable modem termination system (CMTS) routers to include support for both IPv4 and IPv6 protocol stacks.

Note Starting with Cisco IOS Release 12.2(33)SCC and later releases, Cisco CMTS routers also support dual stack on the customer premises equipment (CPE) and IPv6 over subinterfaces.

The IPv6 feature support available in the Cisco IOS software and for Cisco CMTS routers is extensive. This document provides a comprehensive overview of all of the IPv6 features supported on the Cisco CMTS routers, and their restrictions.

However, the details of every feature are not covered in this document. The areas of IPv6 protocol support for the Cisco CMTS routers discussed in this document are classified by platform-independence or by platform-specific feature support.

- Platform-independent IPv6 features—Describes IPv6 features that are supported in the Cisco IOS software for several other Cisco platforms, and which generally do not have any platform-specific behavior or configuration differences on the Cisco CMTS routers.
  - Documentation about the restrictions for these platform-independent features can be found in the Restrictions for IPv6 on Cable, on page 1158.
  - Detailed information about these features, including conceptual and task-based configuration information, is documented outside of this feature and in the Cisco IOS software documentation. Detailed information about the location of this related documentation in the Cisco IOS software documentation is described in the Feature Information for IPv6 on Cable, on page 1207.

- Platform-specific IPv6 features—Describes IPv6 features that are specific to the cable technology area and that only apply to the supported Cisco CMTS routers. The cable-specific IPv6 feature support includes new or modified cable features supporting IPv6, and any transparent support of the IPv6 protocol in existing (legacy) cable features on the CMTS router platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for IPv6 on Cable

- MDF capable line cards are required for DOCSIS 3.0 cable modems (CMs) to support IPv6 CPEs.

Table below shows the hardware compatibility prerequisites for the IPv6 on Cable feature.

Table 120: IPv6 on Cable Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards and SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[76] • Cisco Wideband SPA 2 **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[77] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2 **Cisco IOS Release 12.2(33)SCH and later** • Cisco Next Generation Wideband SPA
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2[78]	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X 1 **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2 3	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X 1 **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2

76 Supports only DOCSIS 2.0 and IPv6 cable modems.
77 Supports only DOCSIS 3.0 and IPv6 cable modems.
78 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2

Note In a typical customer configuration, the IPv6 requires an additional pass through the PRE4. For example, if a packet with a given set of configured features takes one pass through PXF for IPv4 processing, it requires two passes for IPv6 processing.

Restrictions for IPv6 on Cable

The following capabilities are not supported by IPv6 on the Cisco CMTS routers:

- IPv6 support for SCF releases—Cisco IOS SCF releases do not support IPv6 related features

Note Do not enable IPv6 on Cisco IOS SCF releases.

- Access Control List (ACL) extensions for mobile IPv6
- Alternative Provisioning Mode (APM) and Dynamic Provisioning Mode (DPM) (Supported from Cisco IOS Release 12.3(33)SCB onwards)
- Cable Intercept (PacketCable Communications Assistance for Law Enforcement Act [CALEA])
- Cable monitoring based on IPv6 ACL
- Configuration file generation for Dynamic Message Integrity Check (DMIC) for IPv6 cable modems
- DOCSIS Set-top Gateway (DSG) for IPv6
- Hot Standby Router Protocol (HSRP) for IPv6
- Internet Control Message Protocol for IPv6 (ICMPv6) filtering and policing (ICMPv6 is subject to Divert Rate Limit [DRL] in PRE4 punt path.)
- IPv6 anycast addressing
- IPv6 default router preference (DRP)
- IPv6 high availability (HA)
- IPv6 Policy Based Routing (PBR)
- IPv6 VPNs
- Load balancing used with Hot Standby Connection-to-Connection Protocol (HCCP)
- Mobile IPv6 home agent
- Multiple Dynamic Host Configuration Protocol for IPv6 (DHCPv6) addresses

Note Starting with Cisco IOS Release 12.2(33)SCG1, assignment of multiple IPv6 addresses and IPv6 prefixes via DHCP to a single CPE is supported.

- Multi protocol Label System-Virtual Private Network (MPLS-VPN)
- Netflow for IPv6
- Network Address Translation-Protocol Translation (NAT-PT)
- PacketCable and PacketCable Multimedia

Note Starting with Cisco IOS Release 12.2(33)SCJ, IPv6 PacketCable Multimedia Voice is supported.

- Quality of Service (QoS) for IPv6
- Scalable differential IP address assignment (DOCSIS 3.0 assignment of different prefixes to CM and CPE based on DHCPv6 MAC address)

Note Starting with Cisco IOS Release 12.2(33)SCF4, DOCSIS 3.0 assignment of different prefixes to CM and CPE is supported.

- Service Independent Intercept (SII) or Packet Intercept IPv6 address tapping

Note Starting with Cisco IOS Release 12.2(33)SCE, IPv6 HA is supported.

Other restrictions for IPv6 on cable:

DHCPv6 Restrictions for IPv6 on Cable

- Deploy IPv6 source verification only with DHCPv6 leasequery to recover lost CPE data and ensure that traffic from legitimate CPEs can continue to be forwarded.
- DHCPv6 leasequery does not support CPEs that use only prefix delegation (PD) addresses.

The following DHCPv6 areas are not supported by the Cisco CMTS routers:

- DHCP leasequeries
- The following DHCPv6 relay agent options are not supported by the Cisco CMTS routers:
  - Syslog server address option
  - CableLabs client configuration
  - DHCPv6 relay agent subscriber-ID option
  - DHCPv6 relay agent RADIUS attribute option
  - RAAN option

IPv6 Access Services Restrictions for IPv6 on Cable

The following areas of IPv6 access services are not supported by the CMTS routers:

- Authorization, authentication, and accounting (AAA) support for Cisco IPv6 vendor-specific attributes (VSA)

- AAA support for RFC 3162 IPv6 Remote Access Dial-In User Service (RADIUS) attributes
- DHCPv6 prefix delegation via AAA
- Point-to-Point Protocol (PPP) over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- Prefix pools
- Remote bridged encapsulation

IPv6 Data Link Layer Restrictions for IPv6 on Cable

The following areas of the IPv6 Data Link Layer are not supported by the Cisco CMTS routers:

- Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) and ATM LAN emulation (LANE)
- Fiber Distributed Data Interface (FDDI)
- Frame Relay PVC13
- Cisco High-Level Data Link Control (HDLC)
- PPP service over Packet over SONET (POS)
- Integrated Services Digital Network (ISDN)
- Serial (synchronous and asynchronous)
- Virtual LANs (VLANs) using Cisco Inter-Switch Link (ISL)
- Dynamic Packet Transport (DPT)

Multicast Restrictions

IPv6 multicast has the following behavior restrictions on the Cisco CMTS routers:

- IPv6 multicast packets on the Cisco uBR10012 universal broadband router are process-switched by the Performance Routing Engines (PRE).
- IPv6 multicast support complies with DOCSIS 2.0 for Cisco uBR10-MC5X20U and Cisco uBR-MC28U cable interface line cards only.
- IPv6 multicast support complies with DOCSIS 3.0 for Cisco uBR-MC3GX60V, Cisco uBR-MC88V, Cisco UBR-MC20X20V interface line cards, and Cisco Wideband SPA only.
- ICMP redirects are not sent to the originating host if the packet is destined for another CPE behind the same CM. All CPE-to-CPE traffic is processed by the Cisco CMTS router.
- IPv6 multicast forwarding is not supported in Parallel Express Forwarding (PXF), therefore, the IPv6 multicast forwarding performance is limited by the Router Processor (RP).

The following areas of IPv6 multicast are not supported by the Cisco CMTS routers:

- Address family support for Multiprotocol Border Gateway Protocol (MBGP)
- Bidirectional Protocol Independent Multicast (PIM)

- Bootstrap router (BSR)
- DOCSIS 3.0 encrypted multicast
- Explicit tracking of receivers
- IPv6 multicast echo
- Multicast Forwarding Information Base (MFIB) display enhancements
- Multicast use authentication and profile support
- PIM embedded rendezvous point
- Protocol Independent Multicast sparse mode (PIM-SM) accept register feature
- Reverse path forwarding (RPF) flooding of bootstrap router (BSR) packets
- Routable address hello option
- Source Specific Multicast (SSM) mapping for Multicast Listener Device (MLD) version 1 SSM
- IPv6 multicast forwarding on the Cisco uBR10012 universal broadband router in Parallel Express Forwarding (PXF)

Provisioning Restrictions for IPv6 on Cable

The following areas of IPv6 provisioning are not supported on the Cisco CMTS routers:

- Preregistration downstream service ID (DSID) notification
- Bonded-Downstream Channel Descriptor (B-DCD) messages
- Multiple DHCPv6 IPv6 addresses per CM or CPE
- Static IP address assignment for CPEs
- Stateless address auto-configuration (SLAAC) address assignment

Note In Cisco IOS Release 12.2(33)SCC and later, static IPv6 addressing for CPE is supported using Source Address Verification (SAV). For more information about SAV, see the Source Address verification section in the *DOCSIS 3.0 Security Specification* guide.

Note Starting with Cisco IOS Release 12.2(33)SCG1, Multiple IAPDs in a Single Advertise feature supports assignment of multiple IPv6 addresses to a Cable Modem (CM) subscriber.

Note Due to restrictions with DSID and B-DCD messaging support in Cisco IOS Release 12.2(33)SCA, DOCSIS 3.0 CMs must operate with DOCSIS 2.0-level functionality.

QoS Restrictions

Effective with , the following fields are supported for theIPv6 downstream classification:

- IPv6 dest addr
- ipv6 src addr
- IPv6 next header
- IPv6 traffic class

Note IPv6 flow label field is not supported.

The following areas of DOCSIS QoS are not supported by the Cisco CMTS routers:

- Upstream IPv6 Type of Service (ToS) overwrite
- Downstream IPv6 classification

Note ToS overwrite, DOCSIS classification, and Modular QoS CLI (MQC) on Gigabit Ethernet are supported on PRE4 from Cisco IOS Release 12.2(33)SCE onwards.

Routing Restrictions for IPv6 on Cable

The following areas of IPv6 routing are not supported by the Cisco CMTS routers:

- Authenticate route injection via Routing Information Protocol (RIP) for IPv6 (RIPng)
- Differential address/prefix assignment for CM and the CPE behind CM

Note Starting with Cisco IOS Release 12.2(33)SCF4, differential prefix assignment for CM and the CPE behind CM is supported.

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPFv3) cannot operate with IPv6 multicast routing. To use OSPF, you must disable the **ipv6 multicast-routing** command on the Cisco CMTS routers.

Services and Management Restrictions for IPv6 on Cable

The following areas of IPv6 services and management are not supported by the Cisco CMTS routers:

- IPv6 general prefixes
- IPv6 IOS firewall, including IOS firewall and FTP application support

Switching Restrictions for IPv6 on Cable

The following areas of IPv6 switching services are not supported by the Cisco CMTS routers:

- Automatic 6to4 tunnels
- Provider edge router over Multiprotocol Label Switching (MPLS) (6PE)
- CEFv6 switched Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels
- CEFv6 switched automatic IPv4-compatible tunnels
- Parallel Express Forwarding (PXF) switching on the Cisco uBR10012 router

Note PXF switching is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

Tunneling Restrictions for IPv6 on Cable

The following areas of IPv6 tunneling services are not supported by the Cisco CMTS routers:

- Automatic 6to4 tunnels
- Automatic IPv4-compatible tunnels
- IPv6 over Universal Transport Interface (UTI) using a Tunnel Line Card
- ISATAP tunnel support
- IPv6 over IPv6 tunnels
- IP over IPv6 Generic Routing Encapsulation (GRE) tunnels
- IPv6 GRE tunnels in Connectionless Network Service (CLNS) networks

Restrictions for IPv6 Dual Stack CPE Support on the CMTS

The IPv6 Dual Stack CPE Support on the CMTS feature in Cisco IOS Release 12.2(33)SCC has the following limitations:

Note These limitations are not applicable for Cisco IOS Release 12.2(33)SCE. PXF acceleration support is available only on PRE4 from Cisco IOS Release 12.2(33)SCE and later releases.

- The CMTS must use DHCPv4 and DHCPv6 to assign both IPv4 and IPv6 addresses to a dual stack CPE client.
- The IPv6 functionality on the Cisco uBR10012 router manages the CM and tests the infrastructure for CPE deployment. Cisco IOS Release 12.2(33)SCC does not support PXF acceleration of IPv6 data packets on the Cisco uBR10012 router platform. IPv6 data packets from CPE devices are handled by the control processor. Hence, the packets per second (pps) rate is limited to a few kpps per CMTS. IPv6 traffic of 3 kpps on PRE2 and 12 kpps on PRE4 produces an acceptable load on the Cisco uBR10012 control processor.

Restrictions for Implementing IPv6 VPN over MPLS

- The maximum number of IPv6 virtual routing and forwarding instances (VRF) that can be supported is 2038 (including the global routing instances).
- Each subinterface on the CMTS requires an address range from the ISP and from the MSO that will will be used to assign addresses for cable modems. These two address ranges must not overlap and must be extensible to support an increased number of subscribers for scalability.
- This feature does not support DHCPv6 over MPLS and IPv6 multicast.

Note Starting with Cisco IOS Release 12.2(33)SCF4, DHCPv6 over MPLS is supported.

Restrictions for Multiple IAPDs in a Single Advertise

- The cable modem can have only one Identity Association for Non-temporary Address (IA_NA). The IA_NA can either be static or assigned via the DHCP.
- The CPE can have multiple Identity Association for Prefix Delegations (IAPDs) via a DHCP.
- The CPE cannot have multiple IA_NAs and IAPDs, both static and assigned via a DHCP at the same time.
- The default maximum number of IPv6 addresses per CPE is 16.
- The router displays all IA_NA and IAPD requests when CPEs send them together in a single request, or IA_NAs are received first followed by IAPDs. If CPEs send IA_NA and IAPD requests separately to the router and IAPD requests are received first followed by IA_NAs, then only IA_NA addresses are visible on the router. All IAPD addresses are automatically cleared.

Information About IPv6 on Cable

This section includes the following topics:

Features Supported from Cisco IOS Release 12.2(33)SCE

The following features are supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards:

- PXF switching
- PXF acceleration of IPv6 data packets
- Source verification of IPv6 packets in PXF
- ACL support for PXF
- ToS overwrite
- DOCSIS classification

- Modular QoS CLI (MQC) on Gigabit Ethernet
- IPv6 DOCSIS RP and LC HA and DCC
- MAC tapping of IPv6 packets
- Equal cost route load balancing of IPv6 packets destined to the backhaul
- IPv6 over IPv4 GRE tunnels

Features Supported from Cisco IOS Release 12.2(33)SCF4

The following features are supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCF4 onwards:

- Assignment of different prefixes to CM and CPE
- DHCPv6 over MPLS-VPN
- DHCPv6 relay prefix delegation VRF awareness

Features Supported from Cisco IOS Release 12.2(33)SCG1

The following features are supported on Cisco CMTS routers from Cisco IOS Release 12.2(33)SCG1 onwards:

- Assignment of multiple IAPDs in a single advertise for each CPE.
- Assignment of multiple IA_NA and IAPD combinations to multiple CPEs behind a CM.
- The default maximum number of IA_NA and IAPD combinations for each cable modem is 16, including link-local addresses.

Features Supported from Cisco IOS Release 12.2(33)SCI1

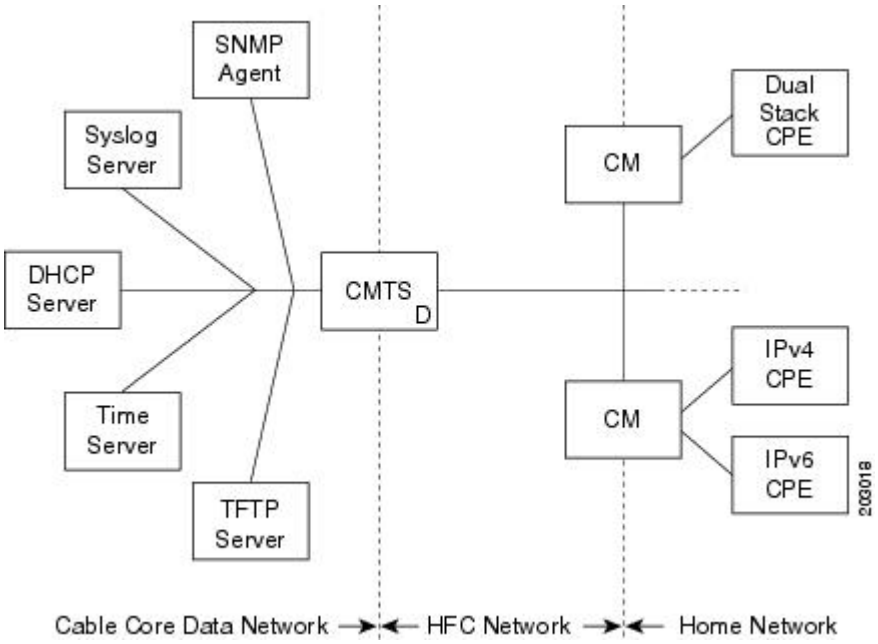
The following features are supported on Cisco CMTS routers from Cisco IOS Release 12.2(33)SCI1 onwards:

- IPv4 and IPv6 Downstream ToS overwrite.
- DHCPv6 Client Link-Layer Address Option (RFC 6939).

Overview of the DOCSIS 3.0 Network Model Supporting IPv6

Figure below illustrates the network model described by the *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*.

Figure 26: DOCSIS 3.0 Network Model



In this model, the different devices support the following functions and services:

- Customer premises equipment (CPE)—Supports IPv4, IPv6, or dual stack operation.

Note In Cisco IOS Release 12.2(33)SCC and later releases, Cisco CMTS routers support CPE devices provisioned for dual stack operation.

- Cable modem (CM)—Functions as a bridging device and supports IPv4, IPv6, or dual stack operation.
- Cable modem termination system (CMTS) router—Works with the CM over the hybrid fiber coaxial cable (HFC) network to provide IPv4 and IPv6 network connectivity to the provisioning servers and the core data network behind the CMTS router.

The CMTS router supports IPv6 address assignment, routing, and forwarding of IPv6 multicast and unicast packets.

Note In Cisco IOS Release 12.2(33)SCA and later releases, the Cisco CMTS router supports only a single DHCPv6 IPv6 address per client CM or CPE. This restriction also applies to DHCPv6 Prefix Delegation prefixes. The reason for blocking more than one DHCPv6 address or prefix for a client is because the end-to-end network requires Source Address Selection (SAS) and all nodes in the end-to-end network may not support the correct SAS. Moreover, the SAS specification (RFC 3484) is being revised by the IETF to define the correct SAS behavior.

- Simple Network Management Protocol (SNMP) agent—Provides management tools to configure and query devices on the network.
- Syslog server—Collects messages from the CM to support its functions.
- Dynamic Host Control Protocol (DHCP) server—The DOCSIS 3.0 network model supports both DHCPv4 and DHCPv6 servers to control the assignment of IP addresses.
- Time server—Provides the current time to the CM.
- Trivial File Transport Protocol (TFTP) server—Provides the CM configuration file.

Note In Cisco IOS Release 12.2(33)SCG1, the Cisco CMTS router supports multiple IPv6 addresses per client CPE via DHCP. The *Multiple IAPDs in a Single Advertise* feature supports assignment of multiple IA_NA and IAPD to a client CPE. This feature removes the restriction introduced in Cisco IOS Release 12.2(33)SCA to enable allocation of multiple globally-reachable IPv6 addresses to home devices of the cable modem subscriber.

Note The Cisco CMTS router supports multiple IPv6 addresses per client CPE via DHCP. The *Multiple IAPDs in a Single Advertise* feature supports assignment of multiple IA_NA and IAPD to a client CPE. This feature removes the restriction introduced in Cisco IOS Release 12.2(33)SCA to enable allocation of multiple globally-reachable IPv6 addresses to home devices of the cable modem subscriber.

Overview of Cable Modem IPv6 Address Provisioning

Prior to cable modem registration with a CMTS router, the CMTS router sends a MAC Domain Descriptor (MDD) message to provide information to the cable modem about its supported IP provisioning mode. You configure the CMTS router provisioning mode using the **cable ip-init** interface configuration command. For more information, see the Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles, on page 1178.

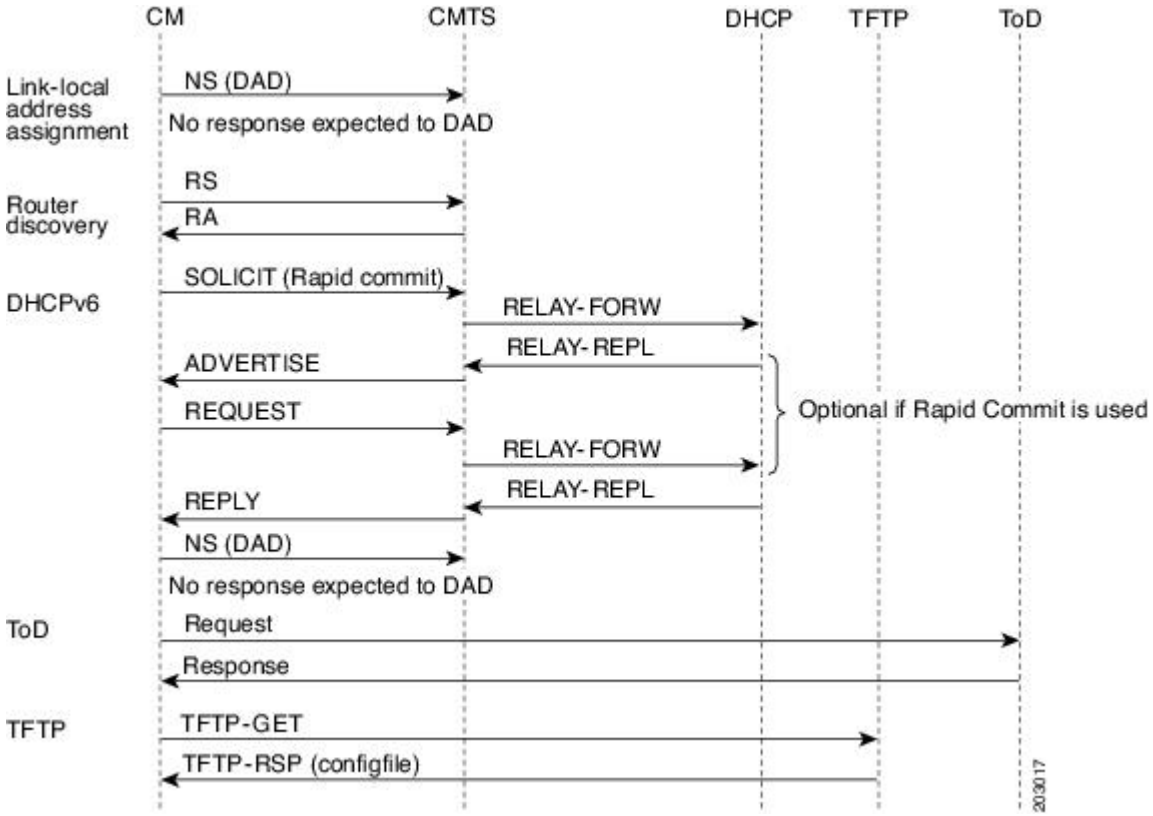
The MDD contains an IP initialization parameters type length value (TLV) that defines the IP version, management and alternate provisioning mode, and pre-registration downstream service ID (DSID) that is used by cable modems that are capable of downstream traffic filtering.

Note In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support alternate provisioning mode or pre-registration DSID.

To support the MULPIv3.0 I04 or later version of the *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*, the cable modem must attempt IPv6 address acquisition first.

Figure below illustrates the message flow between a cable modem, the CMTS router, and the DHCP server when the cable modem is requesting an IPv6 address.

Figure 27: Message Flow for CM Provisioning of DHCP IPv6 Address Assignment



1. Link-local address assignment—The cable modem sends a Neighbor Solicit (NS) message with its link-local address (LLA) to the CMTS router, which starts the duplicate address detection (DAD) process for that LLA. The cable modem expects no response to the NS message.
2. Router discovery—The cable modem listens to the downstream to detect periodical Router Advertise (RA) messages. When an RA message is detected, the cable modem uses the data in the RA message to configure the default route. If an RA is not detected in a specified period, the cable modem sends a Router Solicit (RS) message to find the router on the link (all nodes multicast). The CMTS router responds with a Router Advertise (RA) message with theM and O bits set to 1 to instruct the CM to perform stateful address configuration.

Note Cisco CMTS routers do not support SLAAC address assignment.

- DHCPv6—The cable modem sends a DHCPv6 Solicit message to the CMTS router to request an IPv6 address. The CMTS router relays this message to the DHCPv6 servers. The DHCPv6 servers send an Advertise message indicating the server's availability.

If the Rapid-Commit option is not used by the cable modem, then the cable modem responds to the Advertise message of the server with a Request message to select the server that the CMTS router relays to the DHCPv6 server. If the Rapid-Commit option is used, then multiple DHCPv6 servers that could assign different addresses to the same CPE must not be used.

The cable modem starts the DAD process to verify the uniqueness of the IPv6 address that the DHCPv6 server assigns to it.

- TFTP and Time of Day (ToD)—Once the CM establishes IP connectivity, it sends a request to the TFTP server to download a configuration file and requests the current time from the ToD server to complete its boot process.

Overview of IPv6 Dual Stack CPE Support on the CMTS

In Cisco IOS Release 12.2(33)SCA and later releases, IPv6 was added to the CMTS. Most operating systems (OS) deployed at homes support dual stack operation. In Cisco IOS Release 12.2(33)SCC and later releases, CMTS also supports dual stack, which is both IPv4 and IPv6 addressing on the CPE.

Overview of IPv6 over Subinterfaces

In Cisco IOS Release 12.2(33)SCC, CMTS supports IPv6 over bundle subinterfaces. To configure IPv6 on bundle subinterfaces, see the Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles, on page 1178 section. For a CMTS bundle configuration example, see the Example: IPv6 over Subinterfaces , on page 1193 section.

To enable IPv6 on subinterfaces, configure IPv6 on bundle subinterfaces and not the bundle. Reset the CMs after the subinterface is configured.

Note In Cisco IOS Release 12.2(33)SCC, MPLS VPN over subinterfaces for IPv6 is not supported.

Overview of High Availability on IPv6

In Cisco IOS Release 12.2(33)SCE, CMTS supports HA features on IPv6. IPv6 HA is supported on PRE2 with IPv6 punt path forwarding and on PRE4 with IPv6 PXF forwarding.

Note IPv6 DOCSIS HA and HCCP is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

The IPv6 HA feature support in Cisco CMTS routers covers the following capabilities:

- DOCSIS PRE HA
- DOCSIS line card HA
- Dynamic Channel Change (DCC)

DOCSIS PRE HA

The DOCSIS PRE HA has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

- The CMs and CPEs should not go offline after a PRE switchover.
- The data structures of the IPv6 CM and CPE should be synchronized to the standby PRE before the PRE switchover. Both dynamic and bulk synchronization is supported.
- Single stack, dual stack, and APM are supported for the CM.
- Single stack and dual stack provisioning modes are supported on the CPE.
- After a PRE switchover, the IPv6 neighbor entries are rebuilt by Neighbor Discovery (ND) messages on the standby PRE, and the IPv6 routes are rebuilt after converging the routing protocol.

DOCSIS Line Card HA

The DOCSIS line card HA has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

- The data structures of the IPv6 CM and CPE should be synchronized to the standby line card before the line card switchover. Both dynamic and bulk synchronization is supported.
- The CMs and CPEs should not fall offline after a line card switches over and reverts; the CMs and CPEs should behave the same as before the switchover.
- The DOCSIS line card HA supports both 4+1 and 7+1 redundancy.
- Traffic outages in IPv6 may be longer because traffic recovery occurs only after converging the routing protocol.

Dynamic Channel Change

The Dynamic Channel Change (DCC) feature is supported on Cisco CMTS routers.

Note The behavior of the DCC for single stack IPv6 CM and CPE, or dual stack CM and CPE is the same as that of a single stack IPv4 CM and CPE.

The IPv6 and IPv4 DCC functionality has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

Narrowband Cable Modem

- If the source and destination MAC domains of the CM are on the same line card, DCC initialization techniques 0, 1, 2, 3, and 4 are used to move the CM and its associated CPE from one upstream or downstream to another; or move the CM and CPE from one upstream and downstream combination to another.
- If the source and destination MAC domains of the CM are on different line cards, you can use only the DCC initialization technique 0 to move the CM and its associated CPE across line cards.

Wideband Cable Modem

- If the source and destination MAC domains of the CM are on the same line card, DCC initialization techniques 0, 1, 2, 3, and 4 are used to move the CM and its associated CPE from one upstream to another.
- If the primary downstream of a CM is changed after DCC, you can use only the DCC initialization technique 0 to move the CM and its associated CPE across line cards.

Overview of IPv6 VPN over MPLS

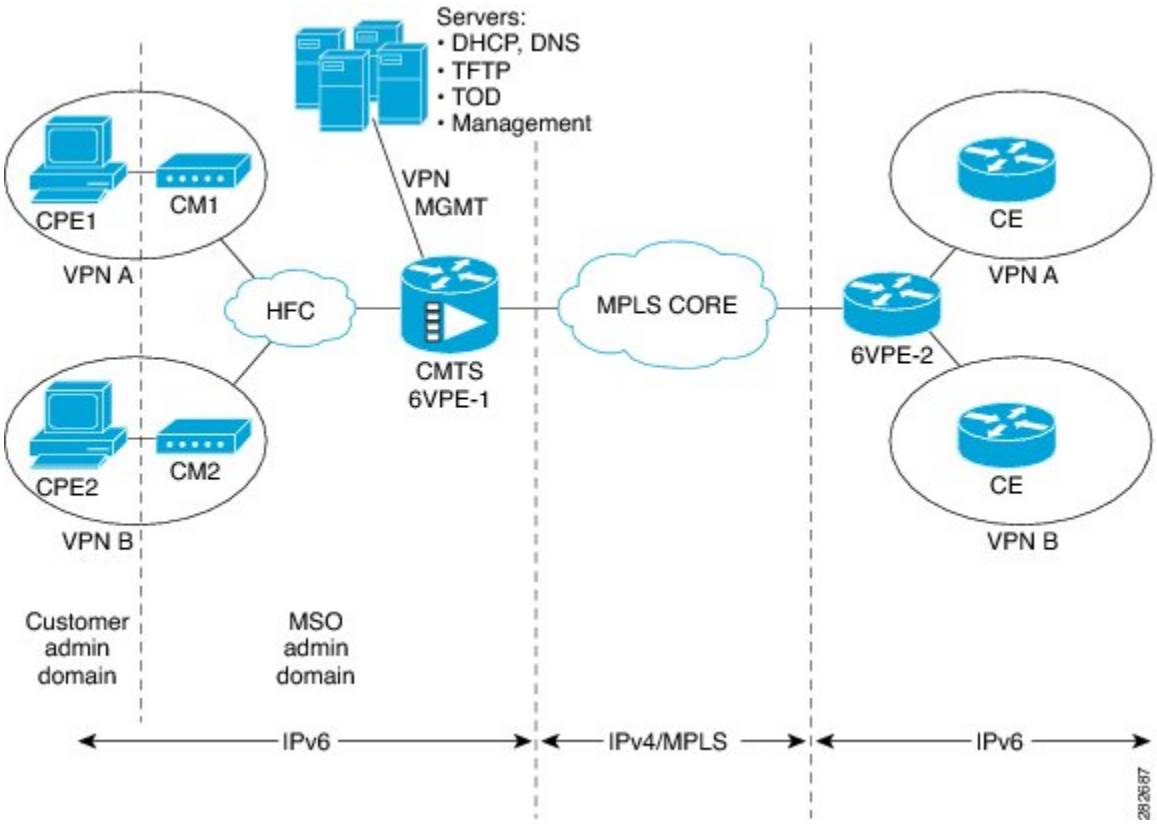
The Multiprotocol Label Switching (MPLS) VPN feature represents an implementation of the provider edge (PE) based VPN model. This document describes the IPv6 VPN over MPLS (6VPE) feature.

The 6VPE feature allows Service Providers to provide an IPv6 VPN service that does not require an upgrade or reconfiguration of the PE routers in the IPv4 MPLS Core. The resulting IPv6 VPN service has a configuration and operation which is virtually identical to the current IPv4 VPN service.

In principle, there is no difference between IPv4 and IPv6 VPNs. In both IPv4 and IPv6, the multiprotocol BGP is the core of the MPLS VPN for IPv6 (VPNv6) architecture. It is used to distribute IPv6 routes over the service provider backbone using the same procedures to work with overlapping addresses, redistribution policies, and scalability issues.

Figure below illustrates the 6PE/6VPE reference architecture diagram.

Figure 28: 6PE/6VPE Reference Architecture



For more information about these tasks, see the Implementing IPv6 VPN over MPLS chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR.

Cable Monitor

The Cable Monitor and Intercept features for Cisco CMTS routers provide a software solution for monitoring and intercepting traffic coming from a cable network. These features give service providers Lawful Intercept capabilities.

For more information, see Cable Monitor and Intercept Features for the Cisco CMTS Routers guide at: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_mon_intrcpt.html

Overview of IPv6 CPE Router Support on the Cisco CMTS

In Cisco IOS Release 12.2(33)SCF and later releases, the IPv6 CPE router support is provided on the Cisco CMTS. The IPv6 CPE router is a node primarily for home or small office use that connects the end-user network to a service provider network. It is also referred to as the home router.

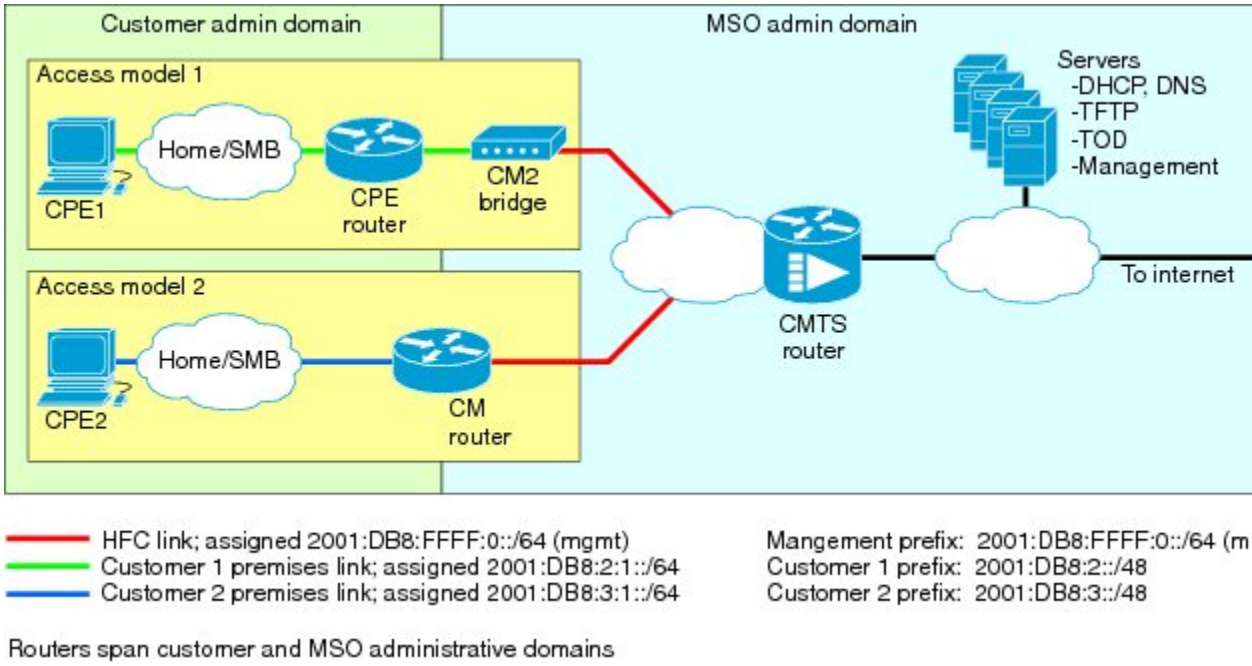
The IPv6 CPE router is responsible for implementing IPv6 routing; that is, the IPv6 CPE router looks up the IPv6 destination address in its routing table and decides to which interface the packet should be sent.

The IPv6 CPE router performs the following functions:

- Provisions its WAN interface automatically.
- Acquires IP address space for provisioning of its LAN interfaces.
- Fetches other configuration information from the service provider network.

Figure below illustrates the CPE router reference architecture diagram between the CPE router, the CMTS, and the DHCPv6 server (CNR) when the CM is requesting an IPv6 address.

Figure 29: IPv6 CPE Router Reference Architecture



As part of the IPv6 CPE Router Support feature, the following enhancements are introduced:

- Support to IPv6 router devices.
- IPv6 Prefix Delegation (PD) High Availability.
- Prefix awareness support in IPv6 cable source-verify, Cable DOCSIS filters code, and packet intercepts.

Support for IPv6 Prefix Stability on the CMTS

Cisco IOS Release 12.2(33)SCF1 supports IPv6 prefix stability on the Cisco CMTS as specified in DOCSIS 3.0 MULPI CM-SP-MULPIv3.0-I15-110210 standard. The IPv6 prefix stability allows an IPv6 home router to move from one Cisco CMTS to another while retaining the same prefix.

The multiple service operators (MSOs) can use this feature to allow their business customers (with IPv6 routers) to retain the same IPv6 prefix during a node split.

Configurable DHCPv6 Relay Address

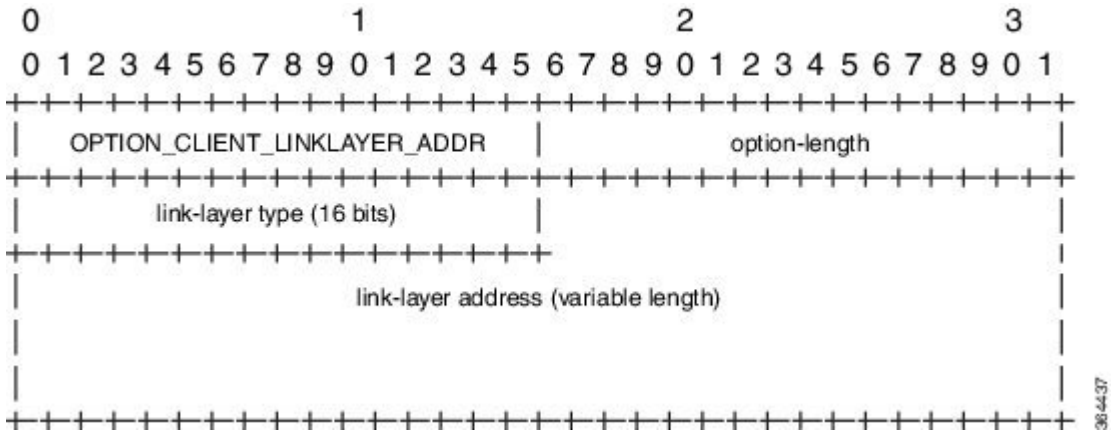
The DHCPv6 Cisco IOS relay agent on the Cisco CMTS router sends relay-forward messages from a source address to all configured relay destinations. The source address is either an IPv6 address provisioned on the network interface or a Cisco CMTS WAN IPv6 address. The relay destination can be a unicast address of a server, another relay agent, or a multicast address. The relay-forward messages contain specific DHCPv6 link-addresses.

A DHCP relay agent is used to relay messages between the client and server. A client locates a DHCP server using a reserved, link-scoped multicast address.

DHCPv6 Client Link-Layer Address Option (RFC 6939)

Cisco IOS Release 12.2(33)SCI1 supports DHCPv6 Client Link-Layer Address Option (RFC 6939). It defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server.

The format of the DHCPv6 Client Link-Layer Address option is shown below.



Name	Description
option-code	OPTION_CLIENT_LINKLAYER_ADDR (79)
option-length	2 + length of MAC address
link-layer type	CPE or CM MAC address type. The link-layer type MUST be a valid hardware type assigned by the IANA, as described in RFC0826.
link-layer address	MAC address of the CPE or CM.

Note Starting with Cisco IOS Release 12.2(33)SCI1, RFC6939 is enabled by default. It can not be enabled/disabled by any CLI command.

To configure DHCPv6 Relay Address on the Cisco CMTS bundle subinterfaces, see the Configuring DHCPv6 Relay Agent, on page 1189 section.

For more information about the DHCPv6 client, server, and relay functions, see the “Implementing DHCP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR .

Unitary DHCPv6 Leasequery

The Cisco IOS Release 12.2(33)SCF1 introduces support for unitary DHCPv6 leasequery protocol (RFC 5007) on the Cisco CMTS routers for upstream IPv6 source verification. This protocol verifies the authenticity of the IPv6 CPE behind a home or small office cable deployment.

For more information on unitary DHCPv6 leasequery, see the Unitary DHCPv6 Leasequery feature guide.

Support for Multiple IAPDs in a Single Advertise

Cisco IOS Release 12.2(33)SCG1supports assignment of multiple IA_NA and IAPD to CPEs behind a CM. This feature includes support for link-local addresses and IA_NA and IAPD. However, a CM can be assigned only one IA_NA. This IA_NA can be either static or DHCP-assigned.

The CPEs behind the CM can request for multiple DHCPv6 IA_NAs and IAPDs. Each CPE is assigned multiple IA_NAs and IAPDs in a single Advertise/Reply message. Each CPE request for IA_NA and IAPD is treated as a separate Advertise/Reply message.

IPv6 Neighbor Discovery Gleaning

The IPv6 Neighbor Discovery (ND) Gleaning feature enables Cisco CMTS routers to automatically recover lost IPv6 CPE addresses and update the CPE records in the Cisco CMTS subscriber database. The Cisco CMTS router gleans only the solicited neighbor advertise (NA) messages transmitted in the upstream direction. IPv6 ND gleaning is similar to Address Resolution Protocol (ARP) gleaning for IPv4 CPE recovery.

The IPv6 ND Gleaning feature is configured by default on Cisco CMTS routers. To disable this feature, use the **no** form of the **cable nd** command in bundle interface configuration mode. The **cable nd** command adds a CPE (host behind a cable modem) to the Cisco CMTS subscriber database. This command does not impact the IPv6 ND protocol operation on the router.

Note The IPv6 ND Gleaning feature does not support gleaning of NA messages transmitted in the downstream direction.

IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept feature provides lawful intercept of cable modems and CPEs provisioned with IPv6 addresses. This feature taps all the packets received and sent from the system. The intercepted packets are sent to the MD with the content connection identifier (CCCID) specified by the tapping rule.

For more information on IPv6 Address Packet Intercept, see the IPv6 Address Packet Intercept feature guide.

How to Configure IPv6 on Cable

This section includes the following tasks:

Configuring IPv6 Switching Services

The CMTS routers support forwarding of unicast and multicast IPv6 traffic using either Cisco Express Forwarding for IPv6 (CEFv6) or distributed CEFv6 (dCEFv6):

- CEFv6—All CMTS platforms
- dCEFv6—Cisco uBR10012 universal broadband router only

The CMTS routers also support Unicast Reverse Path Forwarding (RPF), as long as you enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching globally on the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

To configure forwarding of IPv6 traffic using Cisco Express Forwarding or distributed Cisco Express Forwarding (supported on the Cisco uBR10012 universal broadband router only) on the CMTS routers, you must configure forwarding of IPv6 unicast datagrams using the **ipv6 unicast-routing** global configuration command, and you must configure an IPv6 address on the bundle interface using the **ipv6 address** command.

The **show ipv6 cef platform** command is supported on the Cisco CMTS platform from Cisco IOS Release 12.2(33)SCE onwards. You can use the **show ipv6 cef platform** command for debugging purposes.

Before You Begin

- You must enable Cisco Express Forwarding for IPv4 globally on the router by using the **ip cef** or **ip cef distributed** command before configuring Cisco Express Forwarding v6 or distributed Cisco Express Forwarding v6.

Note The **ip cef** command is enabled by default on all Cisco CMTS routers. Therefore, you only must configure the command if it has been disabled. However, you must explicitly configure the **ip cef distributed** command on a Cisco uBR10012 universal broadband router if you want to run distributed CEF switching services for IPv4 or IPv6.

- You must configure forwarding of IPv6 unicast datagrams using the **ipv6 unicast-routing** global configuration command.
- You must configure IPv6 addressing on the cable bundle interface.
- CEF switching is required for Unicast RPF to work.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **ip cef** • **ip cef distributed** **Example:** `Router(config)# ip cef` `or` `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding. or Enables distributed Cisco Express Forwarding for IPv4 datagrams. **Note** For CMTS routers, distributed Cisco Express Forwarding is supported only on a Cisco uBR10012 universal broadband router.
Step 4	Do one of the following: • **ipv6 cef** • **ipv6 cef distributed** **Example:** `Router(config)# ipv6 cef` `or` `Router(config)# ipv6 cef distributed`	Enables Cisco Express Forwarding v6. or Enables distributed Cisco Express Forwarding v6 for IPv6 datagrams. **Note** For CMTS routers, distributed Cisco Express Forwarding v6 is supported only on a Cisco uBR10012 universal broadband router.
Step 5	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.

What to Do Next

- (Optional) Enable IPv6 multicast routing using the **ipv6 multicast-routing** command in global configuration mode and configure other multicast features.

Note In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support OSPF with IPv6 multicast routing.

Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles

Configuring the Cable Virtual Bundle Interface

The only required IPv6 configuration on a cable line card interface is the IP provisioning mode. The remainder of the IPv6 features are configured at the virtual bundle interface, which is then associated with a particular cable line card interface to establish its configuration.

Most of the IPv6 features that are supported in interface configuration mode (both cable-specific as well as platform-independent IPv6 features) are configured at a cable bundle interface.

The Cisco CMTS routers support IPv6 routing on the bundle interface and map both IPv6 unicast and multicast addresses into the cable bundle forwarding table, for packet forwarding.

Each bundle interface has a unique link-local address (LLA) to support link-local traffic when IPv6 is enabled. Cisco CMTS routers can support a maximum of 40 active bundle interfaces, which also translates to a maximum of 40 active IPv6-enabled bundle interfaces.

Starting with Cisco IOS Release 12.3(33)SCB10, IPv6 commands can be configured on multiple bundle subinterfaces.

Before You Begin

The **cable ipv6 source-verify** and **cable nd** commands are not compatible with each other in Cisco IOS release 12.2(33)SCE and later. You must disable IPv6 ND gleaning using the **no** form of the **cable nd** command before using the **cable ipv6 source-verify** command to ensure that only DHCPv6 and SAV-based CPEs can send traffic on the router.

Restriction All multicast traffic is flooded onto bundle member interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *n* **Example:** `Router(config)# interface bundle 1`	Specifies the cable bundle interface and enters interface configuration mode, where *n* specifies the number of the bundle interface.

	Command or Action	Purpose
Step 4	**ipv6 address***ipv6-prefix*/*prefix-length* [**eui-64**] **Example:** `Router(config-if)# ipv6 address 2001:DB8::/32 eui-64`	Specifies an IPv6 network assigned to the interface and enables IPv6 processing on the interface. The ipv6 address eui-64 command configures site-local and global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. You need to specify only the 64-bit network prefix for the address; the last 64 bits are automatically computed from the interface ID.
Step 5	**ipv6 address***ipv6-prefix* /*prefix-length* **link-local** **Example:** `Router(config-if)# ipv6 address 2001:DB8::/32 link-local`	(Optional) Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface. The **ipv6 address link-local** command configures a link-local address on the interface that is used instead of the link-local address that is automatically configured, when IPv6 is enabled on the interface (using the **ipv6 enable** command).
Step 6	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Automatically configures an IPv6 link-local address on the interface while also enabling the interface for IPv6 processing. The link-local address can be used only to communicate with nodes on the same link.
Step 7	cable ipv6 source-verify **Example:** `Router(config-if)# cable ipv6 source-verify`	(Optional) Enables source verification of MAC address-MD-SID-IPv6 address binding packets received by a cable interface upstream on Cisco CMTS routers. **Note** DHCPv6 leasequery is not supported in Cisco IOS release 12.2(33)SCE.

What to Do Next

- Configure the desired platform-independent IPv6 features on the bundle interface, such as Neighbor Discovery and DHCPv6 features.
- Configure the IP provisioning mode and bundle on the cable interface.

Configuring the IP Provisioning Mode and Bundle on the Cable Interface

The CMTS routers allow you to configure cable interfaces to support cable modems provisioned for both IPv4 and IPv6 addressing support (known as “dual stack”), only IPv4 addressing, or only IPv6 addressing. Prior to cable modem registration, the CMTS router sends its supported provisioning mode to the cable modem in the MDD message.

In addition to configuring the provisioning mode on the cable interface, you must also associate the cable interface with a cable bundle. You perform most of the other IPv6 feature configuration at the bundle interface.

Note This section describes only the commands associated with establishing IPv6 support on a CMTS router. Other cable interface commands that apply but are optional are not shown, such as to configure upstream and downstream features.

Before You Begin

Configuration of a bundle interface is required.

Restriction APM is not supported in Cisco IOS Release 12.2(33)SCA. Support for APM feature is provided from Cisco IOS Release 12.2(33)SCC onwards.

Note Starting from Cisco IOS Release 12.2(33)SCC onwards, the port parameter of the interface cable was changed to *cable-interface-index* to indicate the MAC domain index for the Cisco UBR-MC and Cisco uBR-MC3GX60V cable interface line cards.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot* / *port* | *slot* / *subslot* /*port* } **Example:** `Router(config)# interface cable 5/0/1`	Specifies the cable interface line card, where: The valid values for these arguments are dependent on your CMTS router and cable interface line card. Refer to the hardware documentation for your router chassis and cable interface line card for supported slot and port numbering.
Step 4	**cable ip-init** {**apm** | **dual-stack** | **ipv4** | **ipv6**} **Example:** `Router(config-if)# cable ip-init ipv6`	Specifies the IP provisioning mode supported by the cable interface, where:
Step 5	**cable bundle***n* **Example:** `Router(config)# cable bundle 1`	Associates the cable interface with a configured virtual bundle interface, where *n* specifies the number of the bundle interface.

What to Do Next

- Proceed to configuring any other cable interface features that you want to support, such as upstream and downstream features. For more information about the other cable interface features, refer to the *Cisco IOS CMTS Cable Software Configuration Guide* .
- Proceed to configure other optional IPv6 cable features.

Configuring IPv6 Cable Filter Groups

Cisco IOS Release 12.2(33)SCA extends the CMTS router IPv4 cable filter group capability to add support for IPv6 filter options.

Cable Filter Groups and the DOCSIS Subscriber Management MIB

Cable subscriber management is a DOCSIS 1.1 specification, which can be established using the following configuration methods:

- CMTS router configuration (via CLI)
- SNMP configuration
- DOCSIS 1.1 configuration file (TLVs 35, 36, and 37)

This section describes the IPv6 cable filter group feature support of the packet filtering portion of the DOCSIS Subscriber Management MIB (DOCS-SUBMGMT-MIB) using configuration commands on the CMTS routers. This IPv6 cable filter group support extends filter classifiers with IPv6 addressing options for CM and CPE traffic, but is independent of DOCSIS IPv6 classifiers, which are used to match packets to service flows.

Configuration of IPv6 cable filter groups on the CMTS routers is supported according to the following guidelines:

- A cable filter group consists of a set of **cable filter group** commands that share the same group ID.
- Separate indexes can be used to define different sets of filters for the same group ID. This can be used to define both IPv4 and IPv6 filters to the same filter group.
- CMs can be associated with one upstream and one downstream filter group.
    - Upstream traffic—All traffic coming from CMs is evaluated against the assigned upstream filter group that is configured by the **cable submgmt default filter-group cm upstream** command.
    - Downstream traffic—All traffic going to CMs is evaluated against the assigned downstream filter group that is configured by the **cable submgmt default filter-group cm downstream** command.
- CPEs can be associated with one upstream and one downstream filter group.
    - Upstream traffic—All traffic coming from CPEs is evaluated against the assigned upstream filter group that is configured by the **cable submgmt default filter-group cpe upstream** command.
    - Downstream traffic—All traffic going to CPEs is evaluated against the assigned downstream filter group that is configured by the **cable submgmt default filter-group cpe downstream** command.

Note Because TLVs 35, 36, and 37 do not apply to DOCSIS 1.0 CM configuration files, the only way to enable cable subscriber management for a DOCSIS 1.0 CM is to configure it explicitly on the Cisco CMTS router and activate it by using the **cable submgmt default active** global configuration command.

Before You Begin

You must create the cable filter group before you assign it to a CM or CPE upstream or downstream.

Restriction

- Chained IPv6 headers are not supported.
- An individual filter group index cannot be configured to support both IPv4 and IPv6 versions at the same time. If you need to support IPv4 and IPv6 filters for the same filter group, then you must use a separate index number with the same filter group ID, and configure one index as **ip-version ipv4**, and the other index as **ip-version ipv6**.
- Only a single upstream and a single downstream filter group can be assigned for CM traffic.
- Only a single upstream and a single downstream filter group can be assigned to CPEs attached to a CM such that all CPEs behind a CM share a common filter group.
- For the filter group to work for CMs, a CM must re-register after the CMTS router is configured for the filter group.
- If parallel eXpress forwarding (PXF) is configured on the Cisco uBR10012 router, either the **cable filter group** commands or the interface ACL (**ip access-list**) command can be configured.
- If you do not provision TLVs 35, 36, and 37 in the DOCSIS CM configuration file, then you must activate the functionality by specifying the **cable submgmt default active** global configuration command on the CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable filter group***group-id* **index***index-num***dest-port***port-num*	(Optional) Specifies the TCP/UDP destination port number that should be matched. The valid range is from 0 to 65535. The default value matches all TCP/UDP port numbers (IPv4 and IPv6 filters).

	Command or Action	Purpose
	Example: `Router(config)# cable filter group 1 index 1 dest-port 69`	
Step 4	**cable filter group** *group-id* **index** *index-num* **ip-proto** *proto-type* **Example:** `Router(config)# cable filter group 1 index 1 ip-proto 17`	(Optional) Specifies the IP protocol type number that should be matched. The valid range is from 0 to 256, with a default value of 256 that matches all protocols (IPv4 and IPv6 filters). Some commonly used values are:
Step 5	**cable filter group** *group-id* **index** *index-num* **ip-tos** *tos-mask tos-value* **Example:** `Router(config)# cable filter group 1 index 1 ip-tos 0xff 0x80`	(Optional) Specifies a ToS mask and value to be matched (IPv4 and IPv6 filters): The *tos-mask* is logically ANDed with the *tos-value* and compared to the result of ANDing the *tos-mask* with the actual ToS value of the packet. The filter considers it a match if the two values are the same. The default values for both parameters matches all ToS values.
Step 6	**cable filter group** *group-id* **index** *index-num* **ip-version ipv6** **Example:** `Router(config)# cable filter group 1 index 1 ip-version ipv6`	Specifies that this filter group is an IPv6 filter group.
Step 7	**cable filter group** *group-id* **index** *index-num* **match-action** {**accept** | **drop**} **Example:** `Router(config)# cable filter group 1 index 1 match-action drop`	(Optional) Specifies the action that should be taken for packets that match this filter (IPv4 and IPv6 filters):
Step 8	**cable filter group** *group-id* **index** *index-num* **src-port** *port-num* **Example:** `Router(config)# cable filter group 1 index 1 src-port 50`	(Optional) Specifies the TCP/UDP source port number that should be matched. The valid range is from 0 to 65535. The default value matches all TCP/UDP port numbers (IPv4 and IPv6 filters).
Step 9	**cable filter group** *group-id* **index** *index-num* **status** {**active** | **inactive**} **Example:** `Router(config)# cable filter group 1 index 1 status inactive`	(Optional) Enables or disables the filter (IPv4 and IPv6 filters): **Note** You must create a filter group using at least one of the other options before you can use this command to enable or disable the filter.

	Command or Action	Purpose
Step 10	**cable filter group** *group-id* **index** *index-num* **tcp-flags** *flags-mask flags-value* **Example:** `Router(config)# cable filter group 1 index 1 tcp-flags 0 0`	(Optional) Specifies the TCP flag mask and value to be matched (IPv4 and IPv6 filters):
Step 11	**cable filter group** *group-id* **index** *index-num* **v6-dest-address** *ipv6-address* **Example:** `Router(config)# cable filter group 1 index 1 v6-dest-address 2001:DB8::/32`	(Optional) Specifies the IPv6 destination address that should be matched using the format X:X:X:X::X (IPv6 filters only).
Step 12	**cable filter group** *group-id* **index** *index-num* **v6-dest-pfxlen** *prefix-length* **Example:** `Router(config)# cable filter group 1 index 1 v6-dest-pfxlen 64`	(Optional) Specifies the length of the network portion of the IPv6 destination address. The valid range is from 0 to 128.
Step 13	**cable filter group** *group-id* **index** *index-num* **v6-src-address** *ipv6-address* **Example:** `Router(config)# cable filter group 1 index 1 v6-src-address 2001:DB8::/32`	(Optional) Specifies the IPv6 source address that should be matched using the format X:X:X:X::X (IPv6 filters only).
Step 14	**cable filter group** *group-id* **index** *index-num* **v6-src-pfxlen** *prefix-length* **Example:** `Router(config)# cable filter group 1 index 1 v6-src-pfxlen 48`	(Optional) Specifies the length of the network portion of the IPv6 source address. The valid range is from 0 to 128 (IPv6 filters only).
Step 15	**cable submgmt default filter-group** {**cm** | **cpe**} {**downstream** | **upstream**} *group-id* **Example:** `Router(config)# cable submgmt default filter-group cm upstream 1`	Applies a defined filter group (by specifying its *group-id)* to either a CM or its CPE devices, for downstream or upstream traffic.
Step 16	**cable submgmt default active** **Example:** `Router(config)# cable submgmt default active`	(Required if you do not provision TLVs 35, 36, and 37 in the DOCSIS 1.1 CM configuration file) Enables filters and allows the CMTS to manage the CPE devices for a particular CM (sets the docsSubMgtCpeActiveDefault attribute to TRUE).

The following example shows how to create an IPv6 filter group with ID 254 and an index number of 128. The **ip-version ipv6** keywords must be configured to create the IPv6 filter group; otherwise, the default is an IPv4 filter group:

```
configure terminal
cable filter group 254
 index 128 v6-src-address 2001:DB8::/32
cable filter group 254
 index 128 v6-src-pfxlen 48
cable filter group 254
 index 128 v6-dest-address 2001:DB8::/32
cable filter group 254
 index 128 v6-dest-pfxlen 64
cable filter group 254
 index 128 ip-version ipv6
cable filter group 254
 index 128 match-action drop
cable submgmt default filter-group cm upstream 254
```

This group filters CM upstream traffic and drops any packets with an IPv6 source address of 2001:33::20B:BFFF:FEA9:741F (with network prefix of 128) destined for an IPv6 address of 2001:DB8::/32 (with network prefix of 128).

All of the **cable filter group** commands are associated by their group ID of 254 (and index of 128), and the **cable submgmt default filter-group** command applies the corresponding filter group ID of 254 to CM upstream traffic.

To monitor your cable filter group configuration, use forms of the **show cable filter** command as shown in the following examples. In these output examples, the output from the **show cable filter**, **show cable filter group 254**, and **show cable filter group 254 index 128** commands all display the same information because there is currently only a single filter group and index defined.

Note The "Use Verbose" string appears in the output area of the SrcAddr/mask and DestAddr/Mask fields suggesting use of the **show cable filter group verbose** form of the command to display the complete IPv6 address.

```
Router# show cable filter
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose
        Use Verbose
                                    drop   active
Router# show cable filter group 254
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose        Use Verbose                                     drop   active
Router# show cable filter group 254 index 128
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose        Use Verbose                                     drop   active
Router# show cable filter group 254 index 128 verbose
Filter Group                          : 254
Filter Index                          : 128
Filter Version                        : IPv6
Matches                               : 0
    Source IPv6 address               : 2001:DB8::/32
    Destination IPv6 address          : 2001:DB8::/32
    Match action                      : drop
    Status                            : active
```

Troubleshooting Tips

You should configure the **cable filter group** commands prior to applying a filter group using the **cable submgmt default filter-group** command. Failure to do so results in the following message, and an association to a filter group that is undefined:

```
Router(config)# cable submgmt default filter-group cm upstream 100
Default value set to a nonexistent filter-group 100.
```

Configuring IPv6 Domain Name Service

Cisco IOS Release 12.2(33)SCA introduces the domain name service (DNS) capability for devices using IPv6 addressing on the Cisco CMTS routers.

Cisco IOS Release 12.2(33)SCA introduces the domain name service (DNS) capability for devices using IPv6 addressing on the Cisco CMTS routers.

DNS simplifies the identification of cable devices by associating a hostname with what can often be a complex 128-bit IPv6 address. The hostname can then be used in place of the IPv6 address within the CMTS router CLI that supports use of hostnames.

There are two separate DNS caches supported on a CMTS router—an IOS DNS cache and a cable-specific DNS cache that stores IPv6 addresses learned by the CMTS router for CMs and CPEs.

In this phase of the IPv6 DNS service on cable, the DNS server is queried for domain name information as needed when you use the **show cable modem domain-name** command. When you use this command, the following actions take place:

1. The CMTS router checks whether CMs are online. If a CM is online, the CMTS router uses the corresponding IPv6 address assigned to the CM and looks up its domain name from the IOS DNS cache.
2. If no match is found, the CMTS router sends a DNS-QUERY message with the IPv6 address of the CM to the DNS server, which tries to resolve the domain name.
3. When the DNS reply is received, the CMTS router stores the domain name in the IOS DNS cache for each IPv6 address.
4. The CMTS router also stores the fully-qualified domain name (FQDN) that is replied by the DNS server in the cable-specific DNS cache.

Note Running the **no ip domain lookup** command turns off the DNS resolution.

The following platform-independent Cisco IOS software commands are supported using host names by the CMTS router for IPv6 DNS on cable:

- **connect**
- **ping ipv6**
- **show hosts**
- **telnet**
- **traceroute**

Before You Begin

- A DNS server must be configured.
- You must identify and assign the host names to the IPv6 addresses. If you are using the Cisco DNS server, use the **ip host** global configuration command to map hostnames to IP addresses.
- You must configure the DNS server using the **ip name-server** global configuration command before use of DNS host names (or domains) are available in the supported commands.
- The **show cable modem domain-name** command must be run first on the Route Processor (RP) of the CMTS router before any domain name can be used as part of a cable command.

For more information about configuring these prerequisites and related IP domain configuration options, refer to the *Mapping Host Names to IP Addresses* section in the *Cisco IOS IP Configuration Guide* at: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001317

Restriction

- DNS for cable devices using IPv4 addressing is not supported.
- Due to column size limitations within the command-line interface (CLI), the domain name display is limited to 32 characters. Therefore, the entire domain name cannot always be seen in CMTS router command output.
- Only those cable devices where IPv6 address learning takes place are supported, such as acquiring an IPv6 address through DHCPv6 or the IPv6 (ND) process.
- The cable-specific DNS cache is only updated when you use the **show cable modem domain-name** command on the Route Processor (RP). A DNS-QUERY can only be sent on the RP using this command, therefore the DNS cache cannot update if you use the **show cable modem domain-name** command on a line card console. The output is displayed on the RP only.
- The cable-specific DNS cache does not store partially qualified domain names, only FQDNs are stored.
- The cable-specific DNS cache is not associated with the timeouts that apply to the IOS DNS cache. Therefore, a cable-specific DNS cache entry is not removed when an IOS DNS cache timeout occurs for that device. The cable-specific DNS cache is only updated when you use the **show cable modem domain-name** command.
- The CMTS router supports storage of only one domain name per IPv6 address in the cable-specific DNS cache.
- Domain names for the link local address are not supported.
- The **no ip domain-name** command disables DNS lookup.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*] **Example:** `Router(config)# ip name-server 2001:DB8::/32`	Specifies the address of one or more name servers to use for name and address resolution.
Step 4	**exit** **Example:** `Router(config)# exit`	Leaves global configuration mode and enters privileged EXEC mode.
Step 5	**show cable modem domain-name** **Example:** `Router# show cable modem domain-name`	Updates the cable-specific DNS cache and displays the domain name for all CMs and the CPE devices behind a CM.

Configuring IPv6 Source Verification

Typically, the IPv6 source verification feature is enabled on a cable bundle interface. From there, the cable interface is associated with the virtual bundle interface to acquire its configuration.

When you enable IPv6 source verification on a cable line card interface, the source verification routine verifies the MAC address-MD-SID-IP binding of the packet. If the source verification succeeds, the packet is forwarded. If the verification fails, the packet is dropped.

When a CM is operating as a bridge modem device, then the CMTS router verifies all the IPv6 addresses related to that CM and the CPEs behind that CM.

The **cable ipv6 source-verify** command controls only the source verification of IPv6 packets. For IPv4-based source verification, use the **cable source-verify** command, which also supports different options.

For more information about how to configure IPv6 source verification on a bundle interface, see the Configuring the Cable Virtual Bundle Interface, on page 1178.

Restrictions

Source verification of IPv6 packets occurs only on packets in the process-switched path of the Route Processor (RP).

Note Source verification of IPv6 packets in PXF is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

Configuring IPv6 VPN over MPLS

Starting with Cisco IOS Release 12.2(33)SCF, the Cisco CMTS routers support the IPv6 VPN over MPLS (6VPE) feature. Implementing this feature includes the following configuration tasks.

- Configuring a VRF instance for IPv6
- Binding a VRF to an interface
- Creating a subinterface
- Configuring a static route for PE-to-CE-routing
- Configuring eBGP PE-to-CE routing sessions
- Configuring the IPv6 VPN address family for iBGP
- Configuring route reflectors for improved scalability
- Configuring Internet access

For detailed information about these tasks, see the Implementing IPv6 VPN over MPLS chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sr/ip6-ov-mpls-6vpe.html.

For detailed information about the configuration examples, see Configuration Examples for IPv6 on Cable, on page 1193.

Note Starting from Cisco IOS Release 12.2(33)SCF2, the IPv6 address of the sub-bundle interface (to which the CM is connected) is used in the DHCPv6 relay packet of the CPE DHCPv6 request. If the DHCPv6 packet has to go from one VRF interface to another, the IPv6 address of each VRF interface should be configured on the Cisco CMTS to establish connectivity.

Configuring DHCPv6 Relay Agent

Starting with Cisco IOS Release 12.2(33)SCE5, the Cisco CMTS router supports DHCPv6 relay agent to forward relay-forward messages from a specific source address to client relay destinations.

Perform the steps given below to enable the DHCPv6 relay agent function and specify relay destination addresses on an interface.

Before You Begin

The relay-forward messages should contain specific source IPv6 address. This is required because the firewall deployed between the Cisco CMTS DHCPv6 relay agent and the DHCPv6 server expects only one source address for one Cisco CMTS bundle interface.

Restriction If you change one or more parameters of the **ipv6 dhcp relay destination** command, you have to disable the command using the **no** form, and execute the command again with changed parameters.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface type** *number* **Example:** `Router(config)# interface ethernet 4/2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 dhcp relay destination** *ipv6-address*[*interface*] [**link-address** *link-address*] [**source-address** *source-address*] **Example:** `Router(config-if) ipv6 dhcp relay destination 2001:db8:1234::1 ethernet 4/2 link-address 2001:db8::1 source-address 2001:db8::2`	Specifies a destination address to which client packets are forwarded and enables DHCPv6 relay service on the interface.
Step 5	**end** **Example:** `Router(config-if) end`	Exits interface configuration mode and enters privileged EXEC mode.

Disabling IPv6 ND Gleaning

You must disable IPv6 ND gleaning before configuring IPv6 source verification using DHCPv6 leasequery.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interfacebundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Specifies a bundle interface number and enters bundle interface configuration mode. • *bundle-no* —Bundle interface number. The valid range is from 1 to 255.
Step 4	**no cable nd** **Example:** `Router(config-if) no cable nd`	Disables IPv6 ND gleaning on the Cisco CMTS router.
Step 5	**end** **Example:** `Router(config-if) end`	Returns to privileged EXEC mode.

How to Verify IPv6 Dual Stack CPE Support

This section describes how to use **show** commands to verify the configuration of the IPv6 Dual Stack CPE Support on the CMTS feature in Cisco IOS Release 12.2(33)SCC.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show cable modem** [*ip-address* | *mac-address*] **ipv6**[**cpe** | **prefix** | **registered** | **unregistered]** **Example:** `Router# show cable modem ipv6 registered` **Example:** `Router# show cable modem 0019.474a.c14a ipv6 cpe`	Displays IPv6 information for specified CMs and CPEs behind a CM on a Cisco CMTS router. You can specify the following options:
Step 3	**show cable modem** [ip-address | mac-address] **registered** **Example:** `Router# show cable modem 0019.474e.e4DF registered`	Displays a list of the CMs that have registered with the Cisco CMTS. You can specify the following options:
Step 4	**show cable modem** {ip-address | mac-address} **cpe** **Example:** `Router# show cable modem 0019.474a.c14a cpe`	Displays the CPE devices accessing the cable interface through a particular CM. You can specify the following options:

Examples

Use the **show cable modem ipv6** command to display the IPv6 portion of a dual stack CPE and use the **show cable modem cpe** command to display the IPv4 mode of a dual stack CPE. Both **show cable modem ipv6 registered** and **show cable modem registered** commands display CPE count as one for a dual stack CPE.

The following example shows the output of the **show cable modem ipv6** command:

```
Router# show cable modem ipv6 registered
Interface   Prim Online       CPE IP Address                              MAC Address
            Sid  State
C4/0/U2     1    online       0   ---                                     0019.474a.c18c
C4/0/U2     3    online(pt)   1   2001:420:3800:809:EDA4:350C:2F75:4779   0019.474a.c14a
Router# show cable modem 0019.474a.c14a ipv6 cpe
MAC Address    IP Address                      Domain Name
0005.0052.2c1d 2001:420:3800:809:48F7:3C33:B774:9185
```

Starting from Cisco IOS Release 12.2(33)SCG1, the output of the show cable modem ipv6 command for keyword cpe is changed.

The following example shows the output of the **show cable modem ipv6** command:

```
Router# show cable modem
 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
2001:40:3:4:210:D73B:7A50:2D05
```

The following example shows the output of the **show cable modem registered** command:

```
Router# show cable modem registered
```

```
Interface   Prim Online      Timing Rec   QoS CPE IP address      MAC address
            Sid  State       Offset Power
C4/0/U2     3    online      1022   0.00  2   1   50.3.37.12      0019.474a.c14a
```

The following example shows the output of the **show cable modem cpe** command:

```
Router# show cable modem 0019.474a.c14a cpe

IP address        MAC address      Dual IP
50.3.37.3 0005.0052.2c1d Y
```

Configuration Examples for IPv6 on Cable

This section includes the following examples:

Example: IPv6 over Subinterfaces

The following example shows the CMTS bundle configuration that can be used with subinterfaces:

```
Router# show cable modem ipv6
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type Interface    Mac State    D/IP IP Address
0019.474a.c18c B/D  C4/0/U2      online        Y  2001:420:3800:809:4C7A:D518:91
C6:8A18
Router# show run interface bundle2
Building configuration...
Current configuration : 138 bytes
!
interface Bundle2
 no ip address
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 no cable ip-multicast-echo
end
Router#

show run interface bundle2.1
Building configuration...
Current configuration : 382 bytes
!
interface Bundle2.1
 ip address 50.3.37.1 255.255.255.0
 no cable ip-multicast-echo
 cable helper-address 10.10.0.12
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd prefix default no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval msec 2000
 ipv6 dhcp relay destination 2001:420:3800:800:203:BAFF:FE11:B644
 arp timeout 240
end
```

Example: Basic IPv6 Cable Filter Groups

The following example shows the configuration of an IPv6 filter group that drops traffic from a specific IPv6 host (with source address 2001:DB8::1/48) behind a cable router to an IPv6 host on the network (with destination address 2001:DB8::5/64):

```
configure terminal
!
! Specify the filter group criteria using a common group ID
!
cable filter group 254 index 128 v6-src-address 2001:DB8::1
cable filter group 254 index 128 v6-src-pfxlen 128
cable filter group 254 index 128 v6-dest-address 2001:DB8::5
cable filter group 254 index 128 v6-dest-pfxlen 128
!
! Specify that the filter group is IP version 6
!
cable filter group 254 index 128 ip-version ipv6
!
! Specify the drop action for matching packets
!
cable filter group 254 index 128 match-action drop
!
! Apply the filter group with ID 254 to all CM upstream traffic
!
cable submgmt default filter-group cm upstream 254
```

Example: Complete Cable Configuration with IPv6

The following example shows a complete cable configuration example; it also displays the configuration of multiple cable filter groups using both IPv4 and IPv6 and separate indexes to associate the filter definitions with the same group ID.

```
Router# show running-config
Building configuration...
Current configuration : 15010 bytes
!
! Last configuration change at 08:32:14 PST Thu Nov 8 2007
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service compress-config
!
hostname router
!
boot-start-marker
boot-end-marker
!
enable password password1
!
no aaa new-model
clock timezone PST -9
clock summer-time PDT recurring
clock calendar-valid
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
facility-alarm core-temperature critical 85
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm intake-temperature critical 67
!
```

```
!
card 1/0 2jacket-1
card 1/0/0 24rfchannel-spa-1
card 5/0 5cable-mc520h-d
cable admission-control preempt priority-voice
cable modem vendor 00.18.68 SA-DPC2203
cable modem vendor 00.19.47 SA-DPC2505
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
cable filter group 1 index 1 src-ip 0.0.0.0
cable filter group 1 index 1 src-mask 0.0.0.0
cable filter group 1 index 1 dest-ip 0.0.0.0
cable filter group 1 index 1 dest-mask 0.0.0.0
cable filter group 2 index 1 src-ip 0.0.0.0
cable filter group 2 index 1 src-mask 0.0.0.0
cable filter group 2 index 1 dest-ip 0.0.0.0
cable filter group 2 index 1 dest-mask 0.0.0.0
cable filter group 3 index 1 src-ip 0.0.0.0
cable filter group 3 index 1 src-mask 0.0.0.0
cable filter group 3 index 1 dest-ip 0.0.0.0
cable filter group 3 index 1 dest-mask 0.0.0.0
cable filter group 4 index 1 src-ip 0.0.0.0
cable filter group 4 index 1 src-mask 0.0.0.0
cable filter group 4 index 1 dest-ip 0.0.0.0
cable filter group 4 index 1 dest-mask 0.0.0.0
cable filter group 5 index 1 src-ip 0.0.0.0
cable filter group 5 index 1 src-mask 0.0.0.0
cable filter group 5 index 1 dest-ip 0.0.0.0
cable filter group 5 index 1 dest-mask 0.0.0.0
cable filter group 6 index 1 src-ip 0.0.0.0
cable filter group 6 index 1 src-mask 0.0.0.0
cable filter group 6 index 1 dest-ip 0.0.0.0
cable filter group 6 index 1 dest-mask 0.0.0.0
cable filter group 7 index 1 src-ip 0.0.0.0
cable filter group 7 index 1 src-mask 0.0.0.0
cable filter group 7 index 1 dest-ip 0.0.0.0
cable filter group 7 index 1 dest-mask 0.0.0.0
cable filter group 8 index 1 src-ip 0.0.0.0
cable filter group 8 index 1 src-mask 0.0.0.0
cable filter group 8 index 1 dest-ip 0.0.0.0
cable filter group 8 index 1 dest-mask 0.0.0.0
cable filter group 9 index 1 src-ip 0.0.0.0
cable filter group 9 index 1 src-mask 0.0.0.0
cable filter group 9 index 1 dest-ip 0.0.0.0
cable filter group 9 index 1 dest-mask 0.0.0.0
cable filter group 10 index 1 src-ip 0.0.0.0
cable filter group 10 index 1 src-mask 0.0.0.0
cable filter group 10 index 1 dest-ip 0.0.0.0
cable filter group 10 index 1 dest-mask 0.0.0.0
cable filter group 12 index 1 src-ip 0.0.0.0
cable filter group 12 index 1 src-mask 0.0.0.0
cable filter group 12 index 1 dest-ip 0.0.0.0
cable filter group 12 index 1 dest-mask 0.0.0.0
cable filter group 16 index 1 src-ip 0.0.0.0
cable filter group 16 index 1 src-mask 0.0.0.0
cable filter group 16 index 1 dest-ip 0.0.0.0
cable filter group 16 index 1 dest-mask 0.0.0.0
ip subnet-zero
ip domain name cisco.com
ip host host1 239.192.254.254
ip host host2 239.192.254.253
ip name-server 10.39.26.7
ip name-server 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
!
!
!
ipv6 unicast-routing
ipv6 cef
packetcable multimedia
packetcable
```

```
!
!
!
redundancy
 mode sso
!
!
controller Modular-Cable 1/0/0
 annex B modulation 64qam 0 23
 ip-address 10.30.4.175
 modular-host subslot 5/0
 rf-channel 0 cable downstream channel-id 24
 rf-channel 1 cable downstream channel-id 25
 rf-channel 2 cable downstream channel-id 26
 rf-channel 3 cable downstream channel-id 27
 rf-channel 4 cable downstream channel-id 28
 rf-channel 5 cable downstream channel-id 29
 rf-channel 6 cable downstream channel-id 30
 rf-channel 7 cable downstream channel-id 31
 rf-channel 8 cable downstream channel-id 32
 rf-channel 9 cable downstream channel-id 33
 rf-channel 10 cable downstream channel-id 34
 rf-channel 11 cable downstream channel-id 35
 rf-channel 12 cable downstream channel-id 36
 rf-channel 13 cable downstream channel-id 37
 rf-channel 14 cable downstream channel-id 38
 rf-channel 15 cable downstream channel-id 39
 rf-channel 16 cable downstream channel-id 40
 rf-channel 17 cable downstream channel-id 41
 rf-channel 18 cable downstream channel-id 42
 rf-channel 19 cable downstream channel-id 43
 rf-channel 20 cable downstream channel-id 44
 rf-channel 21 cable downstream channel-id 45
 rf-channel 22 cable downstream channel-id 46
 rf-channel 23 cable downstream channel-id 47
!
!
policy-map foo
policy-map 1
policy-map cos
policy-map qpolicy
policy-map shape
policy-map dscp
!
!
!
!
!
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
!
interface FastEthernet0/0/0
 ip address 10.39.21.10 255.255.0.0
 speed 100
 half-duplex
 ipv6 address 2001:DB8::/32
 ipv6 enable
!
interface Wideband-Cable1/0/0:0
 no cable packet-cache
 cable bonding-group-id 1
!
interface Wideband-Cable1/0/0:1
 no cable packet-cache
 cable bonding-group-id 2
!
interface Wideband-Cable1/0/0:2
 no cable packet-cache
 cable bonding-group-id 3
!
interface Wideband-Cable1/0/0:3
 no cable packet-cache
```

```
 cable bonding-group-id 4
!
interface Wideband-Cable1/0/0:4
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 5
 cable rf-channel 1 bandwidth-percent 60
!
interface Wideband-Cable1/0/0:5
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 6
 cable rf-channel 0 bandwidth-percent 40
 cable rf-channel 2
 cable rf-channel 3
!
interface Wideband-Cable1/0/0:6
 no cable packet-cache
 cable bonding-group-id 7
!
interface Wideband-Cable1/0/0:7
 no cable packet-cache
 cable bonding-group-id 8
!
interface Wideband-Cable1/0/0:8
 no cable packet-cache
 cable bonding-group-id 9
!
interface Wideband-Cable1/0/0:9
 no cable packet-cache
 cable bonding-group-id 33
!
interface Wideband-Cable1/0/0:10
 no cable packet-cache
 cable bonding-group-id 34
!
interface Wideband-Cable1/0/0:11
 no cable packet-cache
 cable bonding-group-id 35
!
interface Cable5/0/0
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 119
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 99000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
```

```
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/1
 cable ip-init ipv6
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 120
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 705000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/2
 no cable packet-cache
 cable downstream channel-id 121
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 8
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 9
```

```
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 10
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 11
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/3
 no cable packet-cache
 cable downstream channel-id 122
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 12
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 13
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 14
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 15
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/4
 no cable packet-cache
 cable downstream channel-id 123
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
```

```
 cable upstream 0 connector 16
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 17
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 18
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 19
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Bundle1
 ip address 10.46.2.1 255.255.0.0 secondary
 ip address 10.46.1.1 255.255.0.0
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 cable dhcp-giaddr policy strict
 cable helper-address 10.39.26.8
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval 5
 ipv6 dhcp relay destination 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
ip default-gateway 10.39.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.39.26.12
ip route 192.168.254.253 255.255.255.255 10.39.0.1
ip route 192.168.254.254 255.255.255.255 10.39.0.1
!
!
no ip http server
no ip http secure-server
!
logging cmts cr10k log-level errors
cpd cr-id 1
nls resp-timeout 1
cdp run
!
tftp-server bootflash:docs10.cm alias docs10.cm
tftp-server bootflash:rfsw_x373.bin alias rfsw_x373.bin
snmp-server community private RW
snmp-server enable traps cable
snmp-server manager
!
!
control-plane
!
!
line con 0
```

```
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
!
cable fiber-node 1
  downstream Modular-Cable 1/0/0 rf-channel 1
  upstream Cable 5/0 connector 0
!
cable fiber-node 2
  downstream Modular-Cable 1/0/0 rf-channel 0 2-3
  upstream Cable 5/0 connector 4
!
end
```

Example: BGP Configuration for 6VPE

The following example shows a sample BGP configuration on CMTS 6VPE.

```
Router# router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 11.1.1.5 remote-as 1
 neighbor 11.1.1.5 update-source Loopback1
 no auto-summary
 !
 address-family vpnv6              --- Enable vpnv6 AF
  neighbor 11.1.1.5 activate      --- Activate neighbor 6VPE-2
  neighbor 11.1.1.5 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf vrf_mgmt
  redistribute connected            ---- Publish directly connected route
  redistribute static
  no synchronization
 exit-address-family
!
 address-family ipv6 vrf vrfa   --- Enable IPv6 vrf AF for each VRF
  redistribute connected
  no synchronization
 exit-address-family
 !
 address-family ipv6 vrf vrfb --- Enable IPv6 vrf AF for each VRF
  redistribute connected
  no synchronization
 exit-address-family
!
```

Example: Subinterface Configuration for 6VPE

The following example shows how to define a subinterface on virtual bundle interface 1.

When configuring IPv6 VPNs, you must configure the first subinterface created as a part of the management VRF. In the following example, Bundle 1.10 is the first sub-interface, which is configured into management VRF. Make sure the CNR server is reachable in management VRF.

```
interface Bundle1.10               --- Management VRF
 vrf forwarding vrf_mgmt
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:110::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
```

```
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.11          --- VRF A
 vrf forwarding vrfa
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:111::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.12          --- VRFB
 vrf forwarding vrfb
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:112::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
```

Example: Cable Interface Bundling

The following example shows how to bundle a group of physical interfaces.

```
int C5/0/4 and int c5/0/3 are bundled.
int c5/0/4
cable bundle 1
int c5/0/3
cable bundle 1
```

Example: VRF Configuration for 6VPE

The following example shows how to create VRFs for each VPN.

```
vrf definition vrf_mgmt
 rd 1:1
 !
 address-family ipv4
 route-target export 1:1
 route-target import 1:1
 route-target import 2:2
 route-target import 2:1
 exit-address-family
 !
 address-family ipv6
 route-target export 1:1
 route-target import 1:1
 route-target import 2:1  -- import route of vrfa
 route-target import 2:2  -- import route of vrfb
 exit-address-family
```

Verifying IPv6 on Cable

This section explains how to verify IPv6 on cable configuration and it contains the following topics:

Verifying IPv6 VRF Configuration

To verify the IPv6 VRF configuration, use the show vrf ipv6 command in privileged EXEC mode.

```
Router# show vrf ipv6 vrfa
  Name                             Default RD          Protocols   Interfaces
  vrfa                             2:1                 ipv4,ipv6   Bu1.11
Router# show vrf ipv6 interfaces
Interface              VRF                              Protocol   Address

Bu1.10                 vrf_mgmt                          up         2001:40:3:110::1
```

```
Fa0/0/0                vrf_mgmt                        up          2001:20:4:1::38

Bu1.11                 vrfa                            up          2001:40:3:111::1

Bu1.12                 vrfb                            up          2001:40:3:112::1

CMTS#
```

Verifying IPv6 BGP Status

To verify the IPv6 BGP status, use the show ip bgp command in privileged EXEC mode.

```
Router# show ip bgp vpnv6 unicast all neighbors

BGP neighbor is 11.1.1.5,  remote AS 1, internal link
  BGP version 4, remote router ID 11.1.1.5
  Session state = Established, up for 00:35:52
  Last read 00:00:37, last write 00:00:14, hold time is 180, keepalive interval is 60 seconds

  BGP multisession with 2 sessions (2 established), first up for 00:40:07
  Neighbor sessions:
    2 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new) on session 1, 2
    Address family IPv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
......
```

Verifying MPLS Forwarding Table

To verify the output of the MPLS forwarding table, use the show mpls forwarding-table command in the privileged EXEC mode.

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
......
19     No Label      2001:40:3:110::/64[V]   \                             ---Route in
vrf_mgmt
                                       0             aggregate/vrf_mgmt
21     No Label      2001:40:3:111::/64[V]   \                             ---Route in
vrfa
                                       0             aggregate/vrfa
22     No Label      2001:40:3:112::/64[V]   \                             ---Route in
vrfb
                                       0             aggregate/vrfb
......
```

Verifying IPv6 Cable Modem and its Host State

To verify IPv6 addresses and connected host states of cable modems and CPEs, use the **show interface cable modem** command in the privileged EXEC mode:

```
Router# show interface cable 7/0/0 modem ipv6
SID  Type State         IPv6 Address                            M MAC address
11   CM  online        2001:420:3800:809:3519:5F9C:B96A:D31    D 0025.2e2d.743a
11   CPE unknown       2001:420:3800:809:3DB2:8A6C:115F:41D8   D 0011.2544.f33b
```

Verifying Multiple IAPDs in a Single Advertise

To verify the multiple IPv6 prefixes assigned to devices on a network, use the show cable modem ipv6 prefix command in privileged EXEC mode:

```
Router# show cable modem ipv6 prefix
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:36:53.075 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
0000.002e.074c R/D  2001:40:1012:8::/64
               R/D  2001:40:2012:1D::/64
0000.002e.074b R/D  2001:40:1012:23::/64
               R/D  2001:40:2012:1C::/64
0000.002e.074a R/D  2001:40:1012:22::/64
               R/D  2001:40:2012:1B::/64
```

To verify the multiple IPv6 prefixes assigned to CPEs behind a CM with a specific MAC address, use the **show cable modem** *mac-address* **ipv6 prefix** command in privileged EXEC mode:

```
Router# show cable modem 0023.bed9.4c8e ipv6 prefix
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:22.335 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
```

To verify the IPv6 information of CPEs behind a CM with a specific MAC address, use the show cable modem *mac-address* ipv6 **cpe** command in privileged EXEC mode:

```
Router# show cable modem 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
               2001:40:3:4:210:D73B:7A50:2D05
```

Additional References

The following sections provide references related to the IPv6 on Cable feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband) routers	Cisco IOS CMTS Cable Command Reference
Platform-independent IPv6 configuration guide	Cisco IOS IPv6 Configuration Guide, Release 12.2SR
Platform-independent IPv6 commands	Cisco IOS IPv6 Command Reference
Platform-independent IPv6 concepts and feature configuration	Cisco IOS IPv6 Configuration Library

Standards

Standard	Title
CM-SP-MULPIv3.0-I04-070518	*DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*
CM-SP-MULPIv3.0-I15-110210	*DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*

MIBs

MIB	MIBs Link
CISCO-IP-FORWARD-MIB CISCO-IP-MIB CISCO-DOCS-EXT-MIB DOCS-CABLE-DEVICE-MIB DOCS-IF-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB IF-MIB (Interface counters) TCP-MIB UDP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
draft-ietf-isis-ipv6-06.txt	*Routing IPv6 with IS-IS*
RFC 2460	*Internet Protocol, Version 6 (IPv6) Specification*
RFC 2461	*Neighbor Discovery for IP version 6 (IPv6)*
RFC 2462	*IPv6 Stateless Address Autoconfiguration*
RFC 2463	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
RFC 2464	*Transmission of IPv6 Packets over Ethernet Networks*
RFC 2710	*Multicast Listener Discovery (MLD) for IPv6*

RFC	Title
RFC 2740	*OSPF for IPv6*
RFC 2893 (Dual stack mode of operation)	*Transition Mechanisms for IPv6 Hosts and Routers*
RFC 3315 (Relay Agent)	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3513	*Internet Protocol Version 6 (IPv6) Addressing Architecture*
RFC 3587	*IPv6 Global Unicast Address Format*
RFC 3596 (AAAA records)	*DNS Extensions to Support IP Version 6*
RFC 3810	*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
RFC 4022	*Management Information Base for the Transmission Control Protocol (TCP)*
RFC 4113	*Management Information Base for the User Datagram Protocol (UDP)*
RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*
RFC 4862	*IPv6 Stateless Address Autoconfiguration*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for IPv6 on Cable

Table below lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 121: Feature Information for IPv6 on Cable

Feature Name	Releases	Feature Information
IPv6 on Cable	12.2(33)SCA	This feature is introduced on the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 Universal Broadband Routers. The following new commands are supported: • **cable ip-init** • **cable ipv6 source-verify** • **clear cable modem name** • **debug cable ipv6** • **show cable modem classifiers** • **show cable modem domain-name** • **show cable modem ipv6** • **show cable modem type**

Feature Name	Releases	Feature Information
	12.2(33)SCA	The following modified commands are supported: • **cable event syslog-server** • **cable filter group** • **clear cable host** • **clear cable modem reset** • **ping docsis** • **show cable filter** • **show cable modem** • **show cable modem access-group**

Feature Name	Releases	Feature Information
IPv6 on Cable (continued)	12.2(33)SCA	• **show cable modem calls** • **show cable modem classifiers** • **show cable modem cnr** • **show cable modem connectivity** • **show cable modem counters** • **show cable modem cpe** • **show cable modem errors** • **show cable modem flap** • **show cable modem mac** • **show cable modem maintenance** • **show cable modem offline** • **show cable modem phy** • **show cable modem qos** • **show cable modem registered** • **show cable modem rogue** • **show cable modem unregistered** • **show interface cable modem** • **show interface cable sid**

Feature Name	Releases	Feature Information
	12.2(33)SCA	The following existing cable features support the IPv6 protocol stack without any other modification to the configuration of the cable feature on the Cisco CMTS routers: • Baseline Privacy Plus (BPI+) • Cable Monitor (Except cable monitoring based on IPv6 ACL) • Cable Transport LAN Service (TLS) • CM configuration files • DHCP Relay Agent option for DOCSIS 3.0, Annex J (See also DHCPv6 Restrictions for IPv6 on Cable, on page 1159)
IPv6 on Cable	12.2(33)SCA	• DMIC (except configuration file generation for DMIC IPv6 CMs) • Dynamic Channel Change (DCC) • DOCSIS Dynamic Service Addition (DSA) and Dynamic Service Change (DSC) operations • DOCSIS load balancing (except load balancing with HCCP) • Flap list • IPv6 L2VPN • Spectrum management • Virtual bundles (See the Configuring the Cable Virtual Bundle Interface, on page 1178)
IPv6 Access Services		

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCP for IPv6 Relay Agent	12.2(33)SCA	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. **Platform-Independent Cisco IOS Software Documentation** The " http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.
IPv6 Access Services: Source Verification	12.2(33)SCA	Enabling IPv6 source verification on a cable line card interface allows the source verification routine to verify the MAC address-MD-SID-IP binding of the packet. If the source verification succeeds, the packet is forwarded. If the verification fails, then the packet is dropped. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 source verification, see the Configuring IPv6 Source Verification, on page 1188.

Feature Name	Releases	Feature Information
IPv6 Access Services: Stateless DHCPv6	12.2(33)SCA	Stateless DHCP for IPv6 allows DHCP for IPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Configuring the Stateless DHCPv6 Function • Configuring the Stateless DHCPv6 Function: Example
IPv6 Basic Connectivity		
Syslog over IPv6	12.2(33)SCA	The Cisco IOS syslog process in IPv6 allows users to log syslog messages to external syslog servers and hosts with IPv6 addresses. **Platform-Independent Cisco IOS Software Documentation** The Simplified IPv6 Packet Header section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter and the Configuring Syslog over IPv6 section of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.

Feature Name	Releases	Feature Information
IPv6 Unicast	12.2(33)SCA	An IPv6 unicast address is an identifier for a single interface, on a single node. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Address Formats • IPv6 Address Type: Unicast • IPv6 Address Type: Multicast • IPv6 Neighbor Solicitation Message • IPv6 Router Advertisement Message • Configuring IPv6 Addressing and Enabling IPv6 Routing

Feature Name	Releases	Feature Information
IPv6 Unicast Reverse Path Forwarding (uRPF)	12.2(33)SCA	The Unicast RPF feature mitigates problems caused by malformed or forged (spoofed) IPv6 source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Prerequisites for Implementing IPv6 Addressing and Basic Connectivity • Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6
IPv6 Cable Filter Groups		

Feature Name	Releases	Feature Information
IPv6 Cable Filter Groups: IPv6 Filter Classifiers for CM and CPE traffic	12.2(33)SCA	The IPv6 cable filter group feature support of the packet filtering portion of the DOCSIS Subscriber Management MIB (DOCS-SUBMGMT-MIB) using configuration commands on the CMTS routers. This IPv6 cable filter group support extends filter classifiers with IPv6 addressing options for CM and CPE traffic, but is independent of DOCSIS IPv6 classifiers which are used to match packets to service flows. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 cable filter groups, see the Configuring IPv6 Cable Filter Groups, on page 1181.
IPv6 Data Link Layer		
IPv6 Data Link: Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet	12.2(33)SCA	In IPv6 networks, a data link is a network sharing a particular link-local prefix. Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet are data links supported for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature: • IPv6 Data Links

Feature Name	Releases	Feature Information
IPv6 Data Link: VLANs Using IEEE 802.1q Encapsulation	12.2(33)SCA	In IPv6 networks, a data link is a network sharing a particular link-local prefix. VLANs using IEEE 802.1Q encapsulation is a type of data link supported for IPv6. **Platform-Independent Cisco IOS Software Documentation** The "IPv6 Data Links" section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 ICMPv6		
ICMPv6	12.2(33)SCA	ICMP for IPv6 generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the MLD protocol for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • ICMP for IPv6 • IPv6 Neighbor Discovery • IPv6 Neighbor Solicitation Message • IPv6 Router Advertisement MessageConfiguring IPv6 ICMP Rate Limiting • IPv6 ICMP Rate Limiting Configuration: Example

Feature Name	Releases	Feature Information
ICMPv6 Redirect	12.2(33)SCA	A value of 137 in the Type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Routers send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Neighbor Redirect Message • IPv6 Redirect Messages
IPv6 Multicast		

Feature Name	Releases	Feature Information
IPv6 Multicast	12.2(33)SCA	An IPv6 multicast address is an identifier for a set of interfaces that typically belong to different nodes. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about the supported IPv6 multicast features on the Cisco CMTS routers: • Prerequisites for Implementing IPv6 Multicast • Restrictions for Implementing IPv6 Multicast • Information about Implementing IPv6 Multicast • Enabling IPv6 Multicast Routing • Configuring the MLD Protocol • Configuring PIM • Configuring Static Mroutes • Disabling Default Features in IPv6 Multicast • Configuration Examples for Implementing IPv6 Multicast • Additional References

Feature Name	Releases	Feature Information
IPv6 Multicast: MLD Access Group	12.2(33)SCA	The MLD access group provides receiver access control in Cisco IOS IPv6 multicast routers. The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • MLD Access Group • Customizing and Verifying MLD on an Interface
IPv6 Multicast: MLD Group Limits	12.2(33)SCA	The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Multicast Listener Discovery Protocol for IPv6 • Implementing MLD Group Limits

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	12.2(33)SCA	PIM-SM uses unicast routing to provide reverse-path information for multicast tree building. PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing IPv6 Multicast • IPv6 Multicast Routing Implementation • Protocol Independent Multicast

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Source Specific Multicast (PIM-SSM)	12.2(33)SCA	PIM-SSM supports the implementation of SSM and is derived from PIM-SM. The SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Multicast Routing Implementation • Protocol Independent Multicast • PIM-Source Specific Multicast • IPv6 Multicast Process Switching and Fast Switching • Configuring PIM
IPv6 Multicast: Scope Boundaries	12.2(33)SCA	IPv6 includes support for global and nonglobal addresses. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Multicast Addressing • Scoped Address Architecture • IPv6 BSR • Configuring a BSR

Feature Name	Releases	Feature Information
IPv6 Multicast: Static Multicast Routing (Mroute)	12.2(33)SCA	IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing IPv6 Multicast • Static Mroutes • Configuring Static Mroutes
IPv6 Neighbor Discovery		
IPv6 Neighbor Discovery	12.2(33)SCA	The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Link-Local Address • ICMP for IPv6 • IPv6 Neighbor Discovery • IPv6 Multicast Groups

Feature Name	Releases	Feature Information
IPv6 Neighbor Discovery Duplicate Address Detection	12.2(33)SCA	IPv6 neighbor discovery duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed). **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Neighbor Solicitation Message • IPv6 Stateless Autoconfiguration
IPv6 Neighbor Discovery Static Cache Entry	12.2(33)SCA	The IPv6 static cache entry for neighbor discovery feature allows static entries to be made in the IPv6 neighbor cache. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature: • IPv6 Neighbor Discovery
IPv6 Routing		

Feature Name	Releases	Feature Information
IPv6 Routing: IS-IS Support for IPv6	12.2(33)SCA	IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IS-IS Enhancements for IPv6 • Configuring Single-Topology IS-IS for IPv6 • Customizing IPv6 IS-IS • Redistributing Routes into an IS-IS Routing Process • Redistributing IPv6 IS-IS Routes Between IS-IS Levels
IPv6 Routing: IS-IS Multitopology Support for IPv6	12.2(33)SCA	IS-IS multitopology support for IPv6 allows IS-IS to maintain a set of independent topologies within a single area or domain. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IS-IS Enhancements for IPv6 • IS-IS Multitopology Support for IPv6 • Transition from Single-Topology to Multitopology Support for IPv6 • Configuring Multitopology IS-IS for IPv6

Feature Name	Releases	Feature Information
IPv6 Routing: Multiprotocol BGP Extensions for IPv6	12.2(33)SCA	Multiprotocol BGP extensions for IPv6 supports the same features and functionality as IPv4 BGP. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Multiprotocol BGP for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Multiprotocol BGP Extensions for IPv6 • How to Implement Multiprotocol BGP for IPv6
IPv6 Routing: Multiprotocol BGP Link-local Address Peering	12.2(33)SCA	IPv6 on Cable supports multiprotocol BGP link-local address peering. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Multiprotocol BGP for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Configuring an IPv6 Multiprotocol BGP Peer Using a Link-Local Address • Multiprotocol BGP Peering Using Link-Local Addresses

Feature Name	Releases	Feature Information
IPv6 Routing: OSPF for IPv6 (OSPFv3)	12.2(33)SCA	OSPF version 3 for IPv6 expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses. **Platform-Independent Cisco IOS Software Documentation** The " Implementing OSPF for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Routing: OSPF for IPv6 Authentication Support with IPSec	12.2(33)SCA	OSPF for IPv6 uses the IPSec secure socket API to add authentication to OSPF for IPv6 packets. **Note** In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support OSPF with IPv6 multicast routing. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing OSPF for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • OSPF for IPv6 Authentication Support with IPSec • Configuring IPSec on OSPF for IPv6 • Defining Authentication on an Interface • Defining Authentication in an OSPF Area

Feature Name	Releases	Feature Information
IPv6 Routing: RIP for IPv6 (RIPng)	12.2(33)SCA	RIP enhancements for IPv6 include support for IPv6 addresses and prefixes, and the use of the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages. **Platform-Independent Cisco IOS Software Documentation** The " Implementing RIP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Routing: Route Redistribution for RIPng	12.2(33)SCA	Routes may be specified by prefix, using a route-map prefix list, or by tag, using the route-map "match tag" function. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing RIP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Redistributing Routes into an IPv6 RIP Routing Process • Configuring Tags for RIP Routes • IPv6 RIP Configuration: Example

Feature Name	Releases	Feature Information
IPv6 Routing: Route Redistribution for IS-IS	12.2(33)SCA	IS-IS for IPv6 supports redistributing routes into an IPv6 IS-IS routing process and redistributing IPv6 IS-IS routes between IS-IS levels. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Information about Implementing IS-IS for IPv6 • Redistributing Routes into an IS-IS Routing Process • Redistributing IPv6 IS-IS Routes Between IS-IS Levels
IPv6 Routing: Static Routes	12.2(33)SCA	Static routes are manually configured and define an explicit path between two networking devices. **Platform-Independent Cisco IOS Software Documentation** The " Implementing Static Routes for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services and Management		

Feature Name	Releases	Feature Information
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	12.2(33)SCA	IPv6 basic connectivity can be enhanced by configuring support for AAAA record types in the DNS name-to-address and address-to-name lookup processes. **Platform-Independent Cisco IOS Software Documentation** The " DNS for IPv6 " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services: Cisco Discovery Protocol—IPv6 Address Family Support for Neighbor Information	12.2(33)SCA	The Cisco Discovery Protocol IPv6 address support for neighbor information feature adds the ability to transfer IPv6 addressing information between two Cisco devices. **Platform-Independent Cisco IOS Software Documentation** The " Cisco Discovery Protocol IPv6 Address Support " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services: CISCO-IP-FORWARD-MIB	12.2(33)SCA	A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. **Platform-Independent Cisco IOS Software Documentation** The " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.

Feature Name	Releases	Feature Information
IPv6 Services: CISCO-IP-MIB Support	12.2(33)SCA	A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. **Platform-Independent Cisco IOS Software Documentation** The " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.
IPv6 Services: DNS Lookups over an IPv6 Transport	12.2(33)SCA	IPv6 supports DNS record types that are supported in the DNS name-to-address and address-to-name lookup processes. **Platform-Independent Cisco IOS Software Documentation** The " DNS for IPv6 " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring DNS for IPv6 on the Cisco CMTS routers, see the Configuring IPv6 Domain Name Service, on page 1186.

Feature Name	Releases	Feature Information
IPv6 Services: IPv6 IPSec VPN	12.2(33)SCA	**Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPSec in IPv6 Security " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Information About Implementing IPSec for IPv6 Security • How to Implement IPSec for IPv6 Security
IPv6 Services: Secure Shell (SSH) Support over IPv6	12.2(33)SCA	SSH in IPv6 functions the same and offers the same benefits as SSH in IPv4—the SSH Server feature enables an SSH client to make a secure, encrypted connection to a Cisco router and the SSH Client feature enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running an SSH server. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • SSH over an IPv6 Transport • Enabling SSH on an IPv6 Router

Feature Name	Releases	Feature Information
IPv6 Services: SNMP over IPv6	12.2(33)SCA	SNMP can be configured over IPv6 transport so that an IPv6 host can perform SNMP queries and receive SNMP notifications from a device running Cisco IOS IPv6. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • SNMP over an IPv6 Transport • Configuring an SNMP Notification Server over IPv6 • Configuring an SNMP Notification Server over IPv6: Examples

Feature Name	Releases	Feature Information
IPv6 Services: Standard Access Control Lists	12.2(33)SCA	Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Traffic Filters and Firewalls for IPv6 Security " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing Traffic Filters and Firewalls for IPv6 Security • Access Control Lists for IPv6 Traffic Filtering • PAM in Cisco IOS Firewall for IPv6 • How to Implement Traffic Filters and Firewalls for IPv6 Security • Configuration Examples for Implementing Traffic Filters and Firewalls for IPv6 Security
IPv6 Switching		

Feature Name	Releases	Feature Information
IPv6 Switching: CEF/dCEF Support	12.2(33)SCA	Cisco Express Forwarding for IPv6 is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed Cisco Express Forwarding for IPv6 performs the same functions as CEFv6 but for distributed architecture platforms. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6 • Configuring Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6 **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 switching on the Cisco CMTS routers, see the Configuring DHCPv6 Relay Agent, on page 1189.
IPv6 Tunneling		

Feature Name	Releases	Feature Information
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels	12.2(33)SCA	A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Overlay Tunnels for IPv6 • IPv6 Manually Configured Tunnels • Configuring Manual IPv6 Tunnels • Configuring Manual IPv6 Tunnels: Example
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	12.2(33)SCA	GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol, but in this case carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Overlay Tunnels for IPv6 • GRE/IPv4 Tunnel Support for IPv6 Traffic • Configuring GRE IPv6 Tunnels • Configure GRE Tunnels: Examples

Feature Name	Releases	Feature Information
IPv6 Tunneling: IPv4 over IPv6 Tunnels	12.2(33)SCA	**Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provide information about this feature: • IPv6 Manually Configured Tunnels • Configuring Manual IPv6 Tunnels
IPv6 Dual Stack CPE Support on the CMTS	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduced this feature on the Cisco CMTS routers. The following sections provide information about this feature: • Restrictions for IPv6 Dual Stack CPE Support on the CMTS, on page 1163 • Overview of IPv6 Dual Stack CPE Support on the CMTS, on page 1169 • How to Verify IPv6 Dual Stack CPE Support , on page 1191
IPv6 over Subinterfaces	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduced this feature on the Cisco CMTS routers. The following sections provide information about this feature: • Overview of IPv6 over Subinterfaces , on page 1169 • Example: IPv6 over Subinterfaces , on page 1193

Feature Name	Releases	Feature Information
IPv6 ND Gleaning	12.2(33)SCC	The IPv6 ND Gleaning feature enables Cisco CMTS routers to automatically recover lost IPv6 CPE addresses. This feature is configured by default on routers. The **cable nd** command was introduced to support this feature. The following sections provide information about this feature: • IPv6 Neighbor Discovery Gleaning, on page 1175 • Disabling IPv6 ND Gleaning, on page 1190
IPv6 Support on Multiple Subinterfaces	12.2(33)SCB10	Starting with Cisco IOS Release 12.2(33)SCB10, IPv6 commands are supported on multiple CMTS bundle subinterfaces.
IPv6 HA	12.2(33)SCE	Cisco IOS Release 12.2(33)SCE introduced this feature on the Cisco CMTS routers.

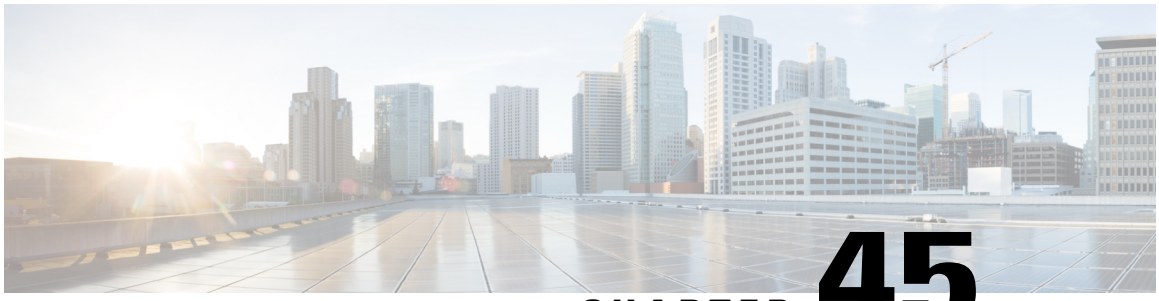
Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Prefix Delegation	12.2(33)SCE3	The DHCP for IPv6 prefix delegation feature can be used to manage link, subnet, and site addressing changes. DHCP for IPv6 can be used in environments to deliver stateful and stateless information. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provide information about this feature: • DHCPv6 Prefix Delegation • Configuring the DHCP for IPv6 Server Function • Configuring the DHCP for IPv6 Client Function • Configuring the DHCP for IPv6 Server Function: Example • Configuring the DHCP for IPv6 Client Function: Example
IPv6: 6PE & 6VPE	12.2(33)SCF	The Multiprotocol Label Switching (MPLS) virtual private network (VPN) feature represents an implementation of the provider edge (PE)-based VPN model. The 6VPE feature allows Service Providers to provide an IPv6 VPN service that does not require an upgrade or reconfiguration of the PE routers in the IPv4 MPLS core. The following sections provide information about this feature: • Overview of IPv6 VPN over MPLS, on page 1171 • Services and Management Restrictions for IPv6 on Cable, on page 1162

Feature Name	Releases	Feature Information
IPv6 CPE Router Support on the Cisco CMTS	12.2(33)SCF	The IPv6 CPE router is a node for home or small office use that connects the end-user network to a service provider network. The following section provides information about this feature: • Overview of IPv6 CPE Router Support on the Cisco CMTS, on page 1172 The following commands were introduced or modified: • show ipv6 route • **show ipv6 cef platform**
Support for IPv6 Prefix Stability on the Cisco CMTS	12.2(33)SCF1	The IPv6 prefix stability on the Cisco CMTS allows an IPv6 home router to move from one Cisco CMTS to another while retaining the same prefix. The following section provides information about this feature: • Overview of IPv6 CPE Router Support on the Cisco CMTS, on page 1172
Unitary DHCPv6 Leasequery protocol (RFC 5007)	12.2(33)SCF1	Added support for RFC 5007 compliant DHCPv6 leasequery protocol. The following commands were introduced or modified: **cable ipv6 source-verify, cable ipv6 source-verify leasequery-filter downstream, show cable leasequery-filter, and debug cable ipv6 lq**.

Feature Name	Releases	Feature Information
Configurable DHCPv6 Relay Address	12.2(33)SCE5	The Cisco CMTS router supports the DHCPv6 relay agent to send relay-forward messages from a specific source address to client relay destinations. The following sections provide information about this feature: **Platform-Specific Documentation for the Cisco CMTS Routers** • Configurable DHCPv6 Relay Address, on page 1173 • Configuring DHCPv6 Relay Agent, on page 1189 The ipv6 dhcp relay destination command was modified for this feature. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provides more information about this feature. • DHCPv6 Client, Server, and Relay Functions

Feature Name	Releases	Feature Information
DHCPv6 with Full 6VPE Support	12.2(33)SCF4	Starting with Cisco IOS Release 12.2(33)SCF4, the following capabilities are supported by IPv6 on the Cisco CMTS routers: • Assignment of different prefixes to CM and CPE • DHCPv6 over MPLS-VPN • DHCPv6 relay Prefix Delegation (PD) VRF awareness The following commands were modified: • **clear ipv6 dhcp relay binding** • **show ipv6 dhcp relay binding** **Platform-Independent Cisco IOS Software Documentation** For more information on the modified commands, see Cisco IOS IPv6 Command Reference .
IPv6 Address Packet Intercept	12.2(33)SCG	The IPv6 Address Packet Intercept feature supports lawful intercept of CMs and CPEs provisioned with IPv6 addresses. The following sections provide information about this feature: • IPv6 Address Packet Intercept • Provisioning IPv6 Taps Using SNMPv3.

Feature Name	Releases	Feature Information
Multiple IAPDs in a Single Advertise	12.2(33)SCG1	The Multiple IAPDs in a Single Advertise feature supports assignment of multiple IA_NAs and IAPDs for a CPE in a single advertise. The output of the **show cable modem ipv6** command was modified to support this feature. The following sections provide more information about this feature: • Restrictions for Multiple IAPDs in a Single Advertise, on page 1164 • Support for Multiple IAPDs in a Single Advertise, on page 1175 • Verifying Multiple IAPDs in a Single Advertise, on page 1204



CHAPTER 45

Multicast VPN and DOCSIS 3.0 Multicast QoS Support

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The CMTS enhanced multicast new features are consistent with DOCSIS 3.0 specifications and include:

- Enhanced multicast echo in which the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table.
- Enhanced multicast quality of service (MQoS) framework that specifies a group configuration (GC) to define a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN).
- Intelligent multicast admission control to include multicast service flows.
- Enhanced multicast VPN feature to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

DOCSIS 1.1 or 2.0 modems are required for multicast encryption.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 122: Multicast VPN and DOCSIS 3.0 Multicast QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [79]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [80]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

79 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

80 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

You can only configure type of service (ToS) for Cisco uBR7200 series universal broadband routers. This parameter is not recognized by the Cisco uBR10012 universal broadband router.

Information About the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

IP multicast—transmission of the same information to multiple cable network recipients—improves bandwidth efficiency and allows service providers to offer differentiated quality of service for different types of traffic. Enhanced multicast introduces multicast improvements as mandated by the introduction of DOCSIS 3.0 specifications.

Note DOCSIS 3.0 standards retain backwards compatibility with the DOCSIS 2.0 multicast mode of operation.

The following are the benefits of CMTS enhanced multicast are:

Improved Multicast Echo

In the enhanced multicast echo feature, the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table instead of the existing multicast echo path. Therefore, upstream packets are echoed using the Layer 3 switching path and all upstream data packets are treated similarly to the ingress packets from a WAN interface, in which they pass through existing classifiers and service flows.

The advantages of improved multicast echo are the following:

- Each outgoing interface has its own DSJIB/DSBlaze header to satisfy baseline privacy interface plus (BPI+) and downstream session identifier (DSID) requirements.
- The echoing decision is based on the PXF multicast routing table with packets forwarded only to interfaces that have existing clients.

- There is independent control of echoing multicast traffic for a single cable interface within a defined cable bundle.
- Bandwidth consumption is reduced because the upstream multicast data packets are not echoed to physical interfaces within the same cable bundle group that do not have an existing client.
- The Internet Group Management Protocol (IGMP) control packets echo functionality is retained allowing the ability to selectively enable or disable multicast echo for IGMP reports and data.
- Multicast QoS is supported because packets are following the same forwarding path as downstream multicast packets.

Enhanced Quality of Service

In the new multicast QoS (MQoS) framework, you can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration (GQC) and a group encryption rule.

Based on the session range, rule priority, and MVPN, a multicast service flow is admitted into a GC and the associated GQC and group encryption rule are applied to the flow. In MQoS implementation, the source address of the multicast session is not checked because the current implementation for cable-specific multicast supports IGMP Version 2 but not IGMP Version 3. The downstream service flow, service identifier (SID), and MAC-rewrite string are created at the time of a new IGMP join (or static multicast group CLI on the interface) and MQoS is applied to the new multicast group join.

The benefits of enhanced QoS are the following:

- Group classifiers can be applied at cable interface level and also at bundle interface level.
- Group service flow (GSF) definition is based on service class names. The GSF is similar to individual service flows and commonly includes the minimum rate and maximum rate parameters for the service class. GSF is shared by all cable modems on a particular downstream channel set (DCS) that is matched to the same group classifier rule (GCR). A default service flow is used for multicast flows that do not match to any GCR. A GSF is always in the active state.
- CMTS replicates multicast packets and then classifies them.
- Single-stage replication and two-stage replication are supported.
- Enhanced QoS is compatible and integrated with DOCSIS Set-Top Gateway (DSG).

Intelligent Multicast Admission Control

Admission control allows you to categorize service flows into buckets. Examples of categories are the service class name used to create the service flow, service flow priority, or the service flow type such as unsolicited grant service (UGS). Bandwidth limits for each bucket can also be defined. For example, you can define bucket 1 for high priority packet cable service flows and specify that bucket 1 is allowed a minimum of 30 percent and a maximum of 50 percent of the link bandwidth.

Intelligent multicast admission control includes additional features such as the inclusion of multicast service flows using the GSF concept. GSFs are created based on the rules as defined in the GQC table. The rules link the multicast streams to a GSF through the session range. The service class name in the rule defines the QoS for that GSF. Additionally, another attribute is added to the rules and the group configuration table to specify the application type to which each GSF belongs. In this way, the QoS associated with each GSF is independent of the bucket category for the GSF.

The benefits of intelligent multicast admission control are the following:

- There is explicit acknowledgment of the establishment of each multicast session.
- Admission control does not consume additional bandwidth for multicast flows once the first flow is established.
- Service flows are cleaned up as the multicast session is torn down.

Multicast Session Limit Support

In a multicast video environment, you can limit the number of multicast sessions admitted onto a particular service flow. The multicast session limit feature—which adds functionality on top of the multicast QoS infrastructure—enables you to specify the number of multicast sessions to be admitted on a particular service flow. If the current number of sessions has reached the defined limit, new sessions will be forwarded but they will make use of the default multicast service flow until a session ends to free up a slot for new sessions.

Multicast Virtual Private Network

The new multicast VPN (MVPN) feature allows you to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment. This feature supports routing and forwarding of multicast packets for each individual VPN virtual routing and forwarding (VRF) instance, and also provides a mechanism to transport VPN multicast packets across the service provider backbone.

MVPN allows you to connect multiple remote sites or devices over either a Layer 3 or Layer 2 VPN. A Layer 3 VPN enables the routing of traffic inside the VPN. A Layer 2 VPN provides a bridging transport mechanism for traffic between remote sites belonging to a customer. To support multicast over Layer 3 VPNs, each VPN receives a separate multicast domain with an associated MVPN routing and forwarding (mVRF) table maintained by the provider edge (PE) router. In a cable environment, the PE router is a routing CMTS. The provider network builds a default multicast distribution tree (default-MDT) for each VPN between all the associated mVRF-enabled PE routers. This tree is used to distribute multicast traffic to all PE routers.

To enable maximum security and data privacy in a VPN environment, the CMTS distinguishes between multicast sessions on the same downstream interface that belong to different VPNs. To differentiate multicast traffic between different VPNs, the CMTS implements a per-VRF subinterface multicast security association identifier (MSAID) allocation feature that is BPI+ enabled. The MSAID is allocated for each cable bundle group for each subinterface. A multicast group has a specific MSAID for each VRF instance.

How to Configure the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

This section contains the following procedures:

Configuring a QoS Profile for a Multicast Group

To configure a QoS profile that can be applied to a QoS group configuration, use the **cable multicast group-qos** command. You must configure a QoS profile before you can add a QoS profile to a QoS multicast group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast group-qos** *number* **scn** *service-class-name* **control**{ **single** | **aggregate** [**limit** *max-sessions*]} **Example:** `Router(config)#: cable multicast group-qos 2 scn name1 control single`	Configures a QoS profile that can be applied to a multicast QoS group. **Note** If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.

Configuring Encryption for a Multicast Group

To configure and enable an encryption profile that can be applied to a QoS group configuration (GC), use the **cable multicast group-encryption** command. You must configure an encryption profile before you can add an encryption profile to a QoS multicast group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number* **algorithm 56bit-des**	Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile.

	Command or Action	Purpose
	Example: `Router(config)#: cable multicast group-encryption 35 algorithm 56bit-des`	• *number*—Enables encryption and specifies the encryption number that can be applied to a specific cable multicast QoS group. The valid range is 1–255. • **algorithm 56bit-des**—Specifies that the data encryption standard (DES) is 56 bits.

Configuring a Multicast QoS Group

You can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration and a group encryption rule.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number***algorithm56bit-des** **Example:** `Router(config-mqos)# cable multicast group-encryption 12 algorithm 56bit-des`	(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile.
Step 4	**cable multicast group-qos** *number* **scn** *service-class-name* **control** {**single** | **aggregate** [limit *max-sessions*]} **Example:** `Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`	(Optional) Configures a QoS profile that can be applied to a multicast QoS group. **Note** If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.

	Command or Action	Purpose
Step 5	**cable multicast qos group** *id* **priority** *value* [**global**] **Example:** `Router(config)# cable multicast qos group 2 priority 6`	Configures a multicast QoS group and enters multicast QoS configuration mode.
Step 6	**session-range** *ip-address ip-mask* **Example:** `Router(config-mqos)# session-range 224.10.10.10 255.255.255.224`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 7	**tos** *low-byte high-byte mask* **Example:** `Router(config-mqos)# tos 1 6 15`	(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for a multicast QoS group.
Step 8	**vrf***name* **Example:** `Router(config-mqos)# vrf name1`	(Optional) Specifies the name for the virtual routing and forwarding (VRF) instance. **Note** If a multicast QoS (MQoS) group is not defined for this VRF, you will see an error message. You must either define a specific MQoS group for each VRF, or define a default MQoS group that can be assigned in those situations where no matching MQoS group is found. See the Configuring a Default Multicast QoS Group for VRF, on page 1250.
Step 9	**application-id***number* **Example:** `Router(config-mqos)# application-id 25`	(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group.

Configuring a Default Multicast QoS Group for VRF

Each virtual routing and forwarding (VRF) instance that is defined must match a defined MQoS group to avoid multicast stream crosstalk between VRFs. To avoid potential crosstalk, define a default MQoS group that is assigned to the VRF whenever the multicast traffic in the VRF does not match an existing MQoS group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number***algorithm56bit-des** **Example:** `Router(config-mqos)# cable multicast group-encryption 12 algorithm 56bit-des`	(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile. The algorithm keyword and 56bit-des argument specify that the data encryption standard (DES) is 56 bits.
Step 4	**cable multicastgroup-qos***number* **scn***service-class-name* **control** {**single** | **aggregate** [**limit** *max-sessions*]} **Example:** `Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`	(Optional) Configures a QoS profile that can be applied to a multicast QoS group.
Step 5	**cable multicast qos group** *id* **priority 255 global** **Example:** `Router(config)# cable multicast qos group 2 priority 255 global`	Configures a default multicast QoS group and enters multicast QoS configuration mode.
Step 6	**session-range 224.0.0.0 224.0.0.0** **Example:** `Router(config-mqos)# session-range 224.0.0.0 224.0.0.0`	Specifies the session-range IP address and IP mask of the default multicast QoS group. By entering 224.0.0.0 for the IP address and the IP mask you cover all possible multicast sessions.
Step 7	**tos***low-byte high-byte mask* **Example:** `Router(config-mqos)# tos 1 6 15`	(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for the default multicast QoS group.
Step 8	**vrf***name* **Example:** `Router(config-mqos)# vrf name1`	Specifies the name of the virtual routing and forwarding (VRF) instance.

	Command or Action	Purpose
Step 9	**application-id***number* **Example:** `Router(config-mqos)# a`**`pplication-id 5`**	(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group.

Verifying Configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

To verify the configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support feature, use the **show** commands described below.

- To show the configuration parameters for multicast sessions on a specific bundle, use the **show interface bundle** *number* **multicast-sessions** command as shown in the following example:

```
Router# show interface bundle 1 multicast-sessions
Multicast Sessions on Bundle1
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Bundle1
 Aggregate Sessions for SAID 8193 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193  ---   1      5   1        Bundle1
```

- To show the configuration parameters for multicast sessions on a specific cable, use the **show interface cable** *ip-addr* **multicast-sessions** command as shown in the following example:

```
Router# show interface cable 7/0/0 multicast-sessions
Default Multicast Service Flow 3 on Cable7/0/0
Multicast Sessions on Cable7/0/0
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Cable7/0/0
 Aggregate Sessions for SAID 8193 SFID 24 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193 24     1      5   1        Bundle1
```

- To show the MSAID multicast group subinterface mapping, use the **show interface cable** *address* **modem** command as shown in the following example:

```
Router# show interface cable 6/1/0 modem
SID   Priv Type      State          IP address      method  MAC address     Dual
      bits                                                                  IP
9     11   modem     online(pt)     101.1.0.6       dhcp    0006.28f9.8c79  N
9     11   host      unknown        111.1.1.45      dhcp    0018.1952.a859  N
10    10   modem     online(pt)     101.1.0.5       dhcp    0006.5305.ac19  N
10    10   host      unknown        111.1.0.3       dhcp    0018.1952.a85a  N
13    10   modem     online(pt)     101.1.0.3       dhcp    0014.f8c1.fd1c  N
```

```
8195  10   multicast unknown        224.1.1.51      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.49      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.50      static  0000.0000.0000  N
```

Configuration Examples for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

This section provides the following configuration examples:

Example: Configuring Group QoS and Group Encryption Profiles

Note To add group QoS and group encryption profiles to a QoS group, you must configure each profile first before configuring the QoS group.

In the following example, QoS profile 3 and encryption profile 35 are configured.

```
configure terminal
cable multicast group-qos 3 scn name1 control single
cable multicast group-encryption 35 algorithm 56bit-des
```

Example: Configuring a QoS Group

In the following example, QoS group 2 is configured with a priority of 6 and global application. To QoS group 2, QoS profile 3 and encryption profile 35 are applied. Other parameters are configured for QoS group 2 including application type, session range, ToS, and VRF.

```
cable multicast qos group 2 priority 6 global
group-encryption 35
group-qos 3
session-range 224.10.10.01 255.255.255.254
tos 1 6 15
vrf vrf-name1
application-id 44
```

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cicso uBR7200 series universal broadband routers, Cisco uBR10012 series universal broadband routers, and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at:

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

Additional References

The following sections provide references related to the Multicast VPN and DOCSIS 3.0 Multicast QoS Support.

Related Documents

Related Topic	Document Title
CMTS cable commands	*Cisco CMTS Cable Command Reference* http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2236	*Internet Group Management Protocol, Version 2*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Table below lists the release history for this feature.

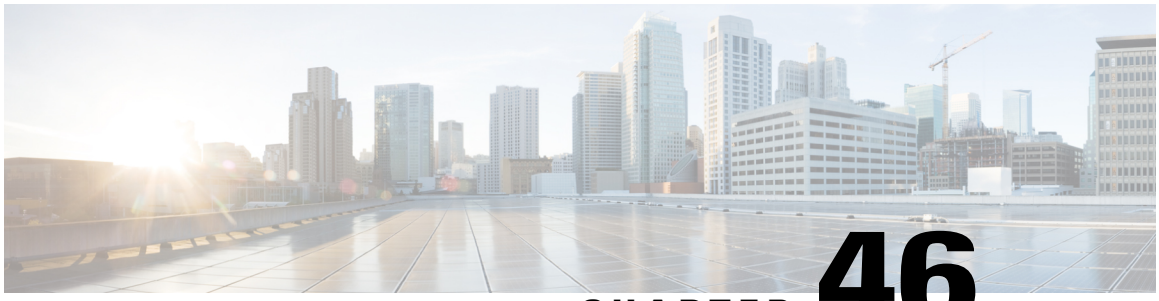
Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 123: Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Feature Name	Releases	Feature Information
Multicast VPN and DOCSIS 3.0 Multicast QoS Support	12.2(33)SCA	Enhanced multicast new features include configuration of a QoS group to include QoS, encryption, VRF, ToS, application type, and session range parameters. The following commands were introduced or modified by this feature: • **application-id** • **cable application-type include** • **cable multicast group-encryption** • **cable multicast group-qos** • **cable multicast qos group** • **session-range** • **show interface bundle multicast-sessions** • **show interface cable modem** • **show interface cable multicast-sessions** • **tos (multicast qos)** • **vrf (multicast qos)**



CHAPTER 46

Virtual Interface Bundling for the Cisco CMTS

First Published: February 11, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to combine multiple cable interfaces in a Cisco Cable Modem Termination System (CMTS) universal broadband router into a single logical bundle, so as to conserve IP address space and simplify network management.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Virtual Interface Bundling

The Virtual Interface Bundling feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SCA. Table below shows the hardware compatibility prerequisites for the Admission Control feature.

Table 124: Virtual Interface Bundling Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [81]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

81 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1.

Information About Virtual Interface Bundling

This section describes the Virtual Interface Bundling feature in Cisco IOS 12.3(13a)BC and later releases, to include configuration, guidelines, examples and additional information in these topics:

Overview of Virtual Interface Bundling

Note In Cisco IOS Release 12.3(21)BC and later releases, all cable bundles are automatically converted and configured to virtual interface bundles. Any standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.

Cisco IOS Release 12.3(13a)BC first introduced support for virtual interface bundling on the Cisco uBR10012 universal broadband router and the Cisco uBR10-MC5X20S/U/H Broadband Processing Engine (BPE), and the Cisco uBR7246VXR router.

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.
- A virtual bundle interface is virtually defined, as with IP loopback addresses.
- Virtual interface bundling supports bundle information in multiple **show** 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**). Prior to Cisco IOS Release 12.3(13a)BC, the Cisco CMTS displays a warning message prior to execution of the **shutdown** command. In Cisco 12.3(13a)BC and later releases, no warning message displays.

Guidelines for Virtual Interface Bundling

The following guidelines describe virtual interface bundling, with comparison to the previous Cable Interface Bundling feature, where applicable:

- The former rules for bundle *master* are applicable to the new *virtual bundle interface* .
- The former rules for bundle *slaves* are applicable to the new virtual bundle *members* .
- With Cisco IOS Release 12.3(13a)BC, initial configuration of the first virtual bundle *member* automatically creates a virtual bundle interface.
- Beginning with Cisco IOS Release 12.3(21)BC, all cable bundles are automatically converted and configured to be in a virtual bundle after loading the software image.
- Beginning with Cisco IOS Release 12.3(21)BC, standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.
- The virtual bundle interface accumulates the counters from members; counters on member links are not cleared when they are added to the bundle. If a bundle-only counter is desired, clear the bundle counter on the members before adding them to the bundle, or before loading the image (for Cisco IOS Release 12.3(21)BC and later).
- Cisco IOS Release 12.3(13a)BC and later releases support a maximum of 40 virtual interface bundles, with the numeric range from 1 to 255.
- In releases prior to Cisco IOS Release 12.3(21)BC, if you delete the virtual bundle interface, the virtual bundle disappears.
- The virtual bundle interface remains configured unless specifically deleted, even if all members in the bundle are deleted.
- This feature supports subinterfaces on the virtual bundle interface.
- *Bundle-aware* configurations are supported on the virtual bundle interface.
- *Bundle-unaware* configurations are supported on each bundle member.
- While creating the virtual bundle interface, if the bundle interface existed in earlier Cisco IOS releases, then the earlier cable configurations re-appear after upgrade.

Virtual Interface Bundle-aware and Bundle-unaware Support

Virtual interface bundling uses two configurations: the virtual *bundle* itself, and the interfaces in that virtual bundle, known as *bundle members* . The virtual interface bundle and bundle members are either aware of the bundle, or unaware of the bundle, as follows.

- Bundle-aware features are maintained on the virtual *bundle* . These include:
  - IP Address
  - IP helper, cable helper
  - Dhcp-giaddr
  - Sub-interface
  - Source verify

- Lease-query
- Address Resolution Protocol (Cable ARP filtering, which also bundles cable interfaces, and Proxy ARP)
- Cable match
- Access Control Lists (ACLs)
- Protocol Independent Multicast (PIM)
- Cable Intercept (supported on the Cisco uBR10012 router with PRE2 module, only)

• Bundle-unaware features are maintained on the *bundle members* . These include:

- DS/US configurations
- HCCP redundancy
- Load balancing
- DMIC, tftp-enforce, shared-secret
- Spectrum management
- Admission control
- Max-host
- Intercept (supported on the Cisco uBR7200 series router and Cisco uBR10012 router with PRE1 module, only)

Multicast Support for IGMPv3 SSM and Virtual Interface Bundling

Cisco IOS Release 12.3(13a)BC introduces support for Internet Group Management Protocol (IGMPv3) Source Specific Multicast (SSM). This enhancement provides support for virtual interface bundling on the Cisco CMTS.

IGMP is used by IPv4 systems to report their IP multicast group memberships to any neighboring multicast routers. The latest IGMPv3 enables an individual member to join a particular channel. This is a new per-channel function, in addition to group-based functions (per-group). This channel based membership is known as Source Specific Multicast (SSM). IGMPv3 SSM allows a multicast client to specify the IP source from which they intend to receive, in addition to normal per-group multicast traffic.

For additional information about using IGMPv3 and virtual interface bundling, refer to enhanced show commands in this document, and to the following document on Cisco.com:

• *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

• *Configuring Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*

http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/feature/guide/mc5x2vif.html

Migrating Bundle Information During a Cisco IOS Upgrade

Migration to virtual interface bundling is automatic the first time a supporting Cisco IOS image is loaded onto the Cisco CMTS.

- Previously configured cable masters and slaves are converted to be members of a new virtual bundle interface.

For cable interface bundling configured in releases prior to Cisco IOS Release 12.3(13a)BC, a new virtual bundle is created with bundle numbers ranging from 1 to 255. However, only a maximum of 40 virtual bundles are supported.

- Bundle-aware configurations are transferred to the virtual bundle interface.
- In releases prior to Cisco IOS Release 12.3(21)BC, you can save new changes, however copying the startup-config to running-config does not translate cable interface bundling to virtual interface bundling, of itself.

Note In Cisco IOS Release 12.3(21)BC and later releases, standalone cable interfaces must be manually configured to be a member of a virtual bundle interface to operate properly.

Configuring Virtual Interface Bundling

Note When upgrading to Cisco IOS Release 12.3(21)BC or later from an earlier release, virtual bundles and bundle members are created and configured automatically. Standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.

When upgrading to Cisco IOS Release 12.3(13a)BC from an earlier release, it may be necessary to reconfigure all cable interface bundling information after loading the Cisco IOS software image. In this circumstance, cable modems do not receive an IP address from the Cisco CMTS until cable interfaces and cable interface bundling is reconfigured.

To enable virtual interface bundling, and to reconfigure interface information on the Cisco CMTS as required, you first configure the virtual interface bundle, then add additional bundle members for the specified virtual bundle. Perform these steps on each interface, as needed for all virtual interface bundles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *n* **Example:** `Router(config-if)# interface bundle 1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. The previous **master** keyword, as supported in the **cable bundle master** command for prior Cisco IOS releases, is not used for virtual interface bundling in Cisco IOS release 12.3(13a)BC, and later releases. As many as 40 virtual interface bundles can be configured on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 7.7.7.7 255.255.255.0`	Use as needed after Cisco IOS upgrade. Configures the IP address for the specified interface and virtual bundle.
Step 5	**interface cable** {*slot* /*port* |*slot* /*subslot* / *port* } **Example:** `Router#` `Router(config-if)#`	Enters interface configuration mode for the selected interface, on which virtual interface bundling is to be enabled. • *slot* /*port* —Cable interface on the Cisco uBR7100 Series or Cisco uBR7200 Series. 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* /*subslot* / *port* — Cable interface on the Cisco uBR10012 router. The following are the valid values: ◦ *slot* —5 to 8 ◦ *subslot* — 0 or 1 ◦ *port* — 0 to 4 (depending on the cable interface)
Step 6	**cable bundle** *n* **Example:** `Router(config-if)# cable bundle 1`	Configures a cable interface to belong to an interface bundle, where *n* is the bundle number.
Step 7	**cable upstream max-ports** *n* **Example:** `Router(config-if)# cable upstream max-ports 6`	Use as needed after Cisco IOS upgrade. Configures the maximum number of upstreams on a downstream (MAC domain) on a Cisco cable interface line card. To reset the card to its default value of 4 upstreams per downstream, use the **no** form of this command. • *n* —Number of upstreams, ranging from 1 to 8, with a default of 4.

	Command or Action	Purpose
Step 8	**cable upstream***logical-port* **connector***physical-port* **Example:** `Router(config-if)# cable upstream 4 connector 16`	Use as needed after Cisco IOS upgrade. Maps an upstream port to a physical port on the Cisco cable interface line card for use with a particular downstream. To remove the mapping and shut down the upstream port, use the **no** form of this command. • *logical-port* —Specifies the upstream port number for the logical port assignment. The number of logical ports is configured with the cable modulation-profile command, and the valid range is from 0 to one less than the current value set with the cable modulation-profile command. **Tip** The default value for max-ports command is 4, which means the default range for logical-port is 0 to 3. • *physical-port* —Specifies the upstream port number for the actual physical port to be assigned. The valid range is 0 to 19, with no default.
Step 9	**cable upstream***n***frequency***up-freq-hz* **Example:** `Router(config-if)# cable upstream 4 frequency 15000000`	Use as needed after Cisco IOS upgrade. Enters a fixed frequency of the upstream radio frequency (RF) carrier for an upstream port. To restore the default value for this command, use the **no** form of this command. • *n* —Specifies the upstream port number on the cable interface line card for which you want to assign an upstream frequency. Valid values start with 0 for the first upstream port on the cable interface line card. • *up-freq-hz* —The upstream center frequency is configured to a fixed Hertz (Hz) value. The valid upstream frequency range is 5 MHz (5000000 Hz) to 42 MHz (42000000 Hz), 55 MHz (55000000 Hz), or 65 MHz (65000000 Hz), depending on the cable interface line card being used. If you wish to have the Cisco CMTS dynamically specify a center frequency for the given upstream interface, do not enter any frequency value.
Step 10	**no cable upstream** *n* **shut** **Example:** `Router(config-if)# no cable upstream 4 shut`	Use as needed after Cisco IOS upgrade. The cable interface must be enabled using the no shutdown command for the specified cable interface. *n* —Specifies the cable interface to enable for the virtual bundle.
Step 11	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

What to Do Next

To remove a virtual bundle from the interface, use the **no interface bundle** command in interface configuration mode, where *n* specifies the bundle identifier:

no interface bundle *n*

If you remove a member from a bundle, the bundle remains on the interface (even if empty) until the bundle itself is specifically removed.

In releases prior to Cisco IOS Release 12.3(21)BC, if you remove a bundle from an interface that still has active members, the bundle is removed.

Monitoring Virtual Interface Bundling

Cisco IOS Release 12.3(13a)BC introduces support for several enhanced show commands that display virtual bundle information.

Example: Virtual Interface Bundling

The following example illustrates a virtual interface bundle with the **show ip interface brief** command:

```
Router# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0/0          1.8.44.1        YES NVRAM  up                    up
POS1/0/0                   unassigned      YES NVRAM  up                    up
GigabitEthernet2/0/0       11.0.0.2        YES NVRAM  up                    up
GigabitEthernet3/0/0       10.1.1.101      YES NVRAM  up                    up
GigabitEthernet4/0/0       1.1.1.1         YES NVRAM  down                  down
Cable8/1/0                 unassigned      YES NVRAM  up                    up
Cable8/1/1                 unassigned      YES NVRAM  up                    up
Cable8/1/2                 unassigned      YES NVRAM  up                    up
Cable8/1/3                 unassigned      YES NVRAM  up                    up
Cable8/1/4                 unassigned      YES NVRAM  up                    up
Bundle1                    10.44.50.1      YES TFTP   up                    up
Router#
```

The following example illustrates virtual bundle information for the specified bundle:

```
Router# show running-config interface Bundle 1
Building configuration...
Current configuration : 189 bytes
!
interface Bundle1
 ip address 10.44.51.1 255.255.255.0 secondary
 ip address 10.44.50.1 255.255.255.0
 ip access-group 130 in
 ip helper-address 1.8.35.200
 cable source-verify dhcp
end
```

The following examples illustrate subinterface information for the specified bundle on a Cisco uBR10012 router:

```
Router# sh ip int br | include Bundle
Bundle1                    10.44.50.1      YES TFTP   up                    up
Bundle150                  unassigned      YES unset  up                    up
Bundle150.1                30.0.0.1        YES manual up                    up
Bundle200                  unassigned      YES unset  up                    up
Bundle255                  unassigned      YES unset  up                    up
Router# sh run int Bundle150.1
Building configuration...
```

```
Current configuration : 93 bytes
!
interface Bundle150.1
 ip address 30.0.0.1 255.0.0.0
 cable helper-address 1.8.35.200
end
```

Additional References

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco IOS CMTS Cable Command Reference Guide

Standards and RFCs

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS

Table below lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

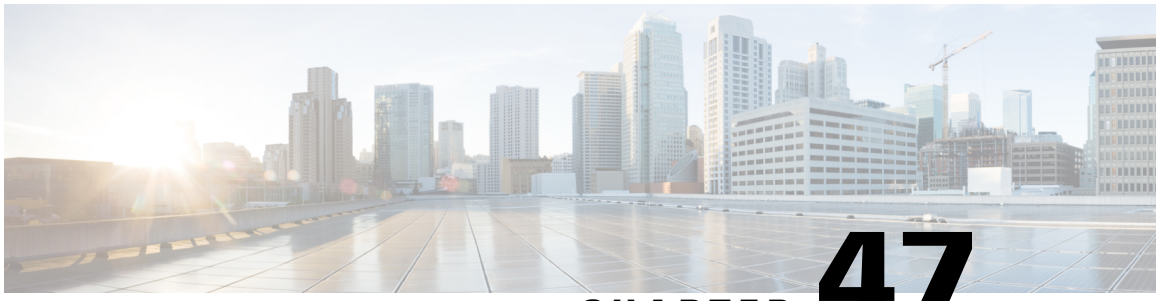
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 125: Feature Information for Bundling on the Cisco CMTS

Feature Name	Releases	Feature Information
Virtual Interface Bundling	12.3(13a)BC	Cable bundling was updated to virtual interface bundling, so that cable bundles are automatically converted to virtual interface bundles. Cable bundling concepts, such as master and slave linecards, are no longer supported. See the Information About Virtual Interface Bundling, on page 1259. In Cisco IOS Release 12.3(21)BC, all cable bundles are now automatically converted and configured to be in a virtual bundle, and standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly. Previously, new virtual interface bundles and bundle members required reconfiguration, and there could also be standalone interfaces not part of a bundle at all.

Feature Name	Releases	Feature Information
Automatic Virtual Interface Bundling	12.2(33)SCA	Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 47

Layer 3 CPE Mobility

First Published: February 18, 2014

Cisco IOS 12.2(33)SCH2 introduces the Layer 3 CPE Mobility feature, which allows the mobility CPE devices to move between cable modems with as less disruption of traffic as possible.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Layer 3 CPE Mobility

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 126: Layer3 CPE Mobility for the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCH2 and later releases • PRE4 • PRE5	**Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [82]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [83]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

82 Cisco uBR3GX60V cable interface line card is compatible with PRE4.
83 Cisco uBR-MC88V cable interface line card is compatible with NPE-G2.

Restrictions for Layer 3 CPE Mobility

- Layer 3 CPE Mobility feature allows CPE devices to move only in the same bundle or sub-bundle interface.
- The IPv4 or IPv6 subnets that are configured with mobility must match with the IPv4 or IPv6 subnets already configured on bundle or sub-bundle interface. Otherwise, configuration will not be accepted and the following message will be displayed:

```
Please remove the previous online CPEs or reset CMs,
```

- If you remove the IPv4 or IPv6 address on bundle or sub-bundle interface, it also removes the relative mobility subnets at the same time.
- Multicast packets will not trigger the Layer 3 CPE Mobility feature.
- VRF configured under bundle or sub-bundle interface is not supported for CPE mobility feature.

- On Cisco uBR72000 series platform, Layer3 CPE Mobility may fail if cable filter is configured.
- On uBR10k series platform, if PXF is disabled, Layer3 CPE Mobility function may not be fully supportd and some behavior may not be consistent with PXF enabled scenario.
- In Layer 3 CPE Mobility feature, the packet lost time period during mobility will be unpredictable, depending on how many CPE devices move at the same time and system loading conditions.
- For CPE devices, which have multiple IPv4 or IPv6 addresses, all of IPv4 or IPv6 addresses will be rebuilt with new source information.
- Layer 3 CPE Mobility may be failed during line card or PRE HA and the trigger upstream packet will be dropped.
- If CPE mobility is turned on, mobility behavior will become effective before cable Ipv4 or IPv6 source verify.
- If Layer 3 CPE Mobility is enabled, some of the security checks will be skipped for the mobility subnets to achieve faster movement of the CPE devices.

Information About Layer 3 CPE Mobility

The Layer 3 CPE Mobility feature allows CPE devices to move from cable modem to other by trigger of any unicast upstream packets of IPv4 or IPV6.

Each cable modem would be situated at a business hotspot location and the CPE devices move from one business location to another, where the service provider is the same and the head end CMTS is the same. This mobility is allowed for selected IP subnets.

The maximum number of subnets supported is 2 IPv6 and 6 IPv4 subnets per bundle or sub-bundle interface. To support more subnets, configure more bundle or sub-bundle interfaces.

The IPv4 or IPv6 subnets that are configured with mobility must match with the IPv4 or IPv6 subnets already configured on bundle or sub-bundle interface. Otherwise, configuration will not be accepted and the following message will be displayed:

```
Please remove the previous online CPEs or reset CMs,
```

When you remove mobility subnets under bundle or sub-bundle interface. The following warning message will be displayed after mobility subnets is configured or removed.

```
Warning: Please remove the previous online CPEs or reset CMs, to make the mobility scope
change works for every device !!!
```

Note If you have enabled mobility configuration for a subnet, the existing online CPE devices will not be aware of the mobility subnets. So after mobility subnets is configured, in order to make the mobility feature work for every CPE device, remove the online CPE devices or reset cable modem.

Benefits of Layer 3 CPE Mobility

The feature provides the movement of CPE devices from one cable modem to another without change in the IP address and the TCP or UDP sessions established are maintained.

How to Configure Layer 3 Mobility

Configuring CPE Mobility

This section describes how to enable mobility on a particular IP subnet on a interface or subinterface bundle.

Before You Begin

Mobility subnets should match the IPv4 or IPv6 address configured on the bundle or sub-bundle interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle bundle number| bundle-subif-number** **Example:** `Router(config)# interface bundle 1` `or` `Router(config)# interface Bundle 1.1`	Enters interface configuration or subinterface mode.
Step 4	**cable l3-mobility** *IP-address mask | IPv6 prefix* **Example:** `Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64` **Example:** `Router(config-subif)# cable l3-mobility 192.0.3.1 255.255.255.0` **Example:** `Router(config-subif)#cable l3-mobility 2001:DB:22:1::1/64`	Enables mobility for a particular IPv4 or IPv6 subnet. **Note** This command can be configured on a interface or a subinterface bundle.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)#` **exit**	Exits interface configuration mode.

What to Do Next

Troubleshooting Tips

If the mobility IP address does not match with the mobility subnet, the following warning message is displayed:

```
Mobility IP should match the IDB subnet!
```

If you remove the IPv4 or IPv6 address from the interface, the mobility scope is removed for the IP address and the following warning message is displayed.

```
IPv6 2001:DBB:3:111::1 removed from Mobility subnets on Bundle1
.
```

Configuring PXF Divert-Limit

This section describes how to configure or modify the PXF divert limit. This procedure is optional and if not configured, will set the value to the default value.

Note If **cable l3 mobility** command on the bundle or sub-bundle interface is enabled, the PXF divert limit is also enabled by default. So this configuration is optional.

Before You Begin

Ensure that the **cable l3 mobility** command is enabled on the bundle or sub-bundle interface. If disabled, the **service divert-limit l3-mobility** function does not work.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>` **enable**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-limit l3-mobility-counter** *limit* | **l3-mobility-timeslot** *timeslot* **Example:** `Router(config-if)# service divert-limit l3-mobility-counter 1` `Router(config-if)# service divert-limit l3-mobility-timeslot 1`	Configures the PXF threshold limit and timslot. • **l3-mobility-counter —** Configures the layer 3 CPE mobility counter threshold limit. • *limit***—** Specifies the mobility counter threshold limit in packets. The default is 16. • **l3-mobility-timeslot —** Configures the layer 3 CPE mobility timeslot in ms. The default is 300. • *timeslot* **—** Specifies the mobility timeslot in milliseconds. The range is from 1 to 4095. The range is from 1 to 127.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits global configuration mode.

Disabling CPE Mobility

This section describes how to disable mobility on a particular IP subnet.

Before You Begin

The CPE mobility should be enabled on a particular IP subnet before you complete this procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface bundle** *bundle number | bundle-subif-number* **Example:** `Router(config)# interface bundle 1` `or` `Router(config)# interface Bundle 1.1`	Enters interface configuration or subinterface mode.
Step 4	**no cable l3-mobility** *IP-address mask | IPv6 prefix* **Example:** `Router(config-if)# cable l3-mobility 192.0.3.1 255.255.255.0` `Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64`	Disbles mobility for a particular IPv4 or IPv6 subnet. **Note** This command can be configured on a interface or a subinterface bundle
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Verifying Layer 3 Mobility Configuration

To verify the layer 3 mobility configuration, use the **show cable bundle** command.

```
Router# show cable bundle 1 mobility Interface                    IP/IPv6 Subnet

-------------------------------------------------------------------------------
Bundle1                    ---
Bundle1.1               192.0.3.0/16
                                192.0.3.1/16
                                192.0.4.1/16
                                2001:DB:5:4:100::1/32
                                2001:DB:5:4:101::1/32
Bundle1.2              192.0.3.1/16
```

Configuration Examples for Layer 3 Mobility

This section provides the following configuration examples:

Example: Configuring CPE Layer 3 Mobility

The following example shows how to configure the layer 3 CPE mobility on a interface bundle:

```
Router#show running interface bundle 10
Building configuration...
Current configuration : 1247 bytes
!
interface Bundle10
```

```
ip address 192.0.3.1 255.255.255.0 secondary
ip address 192.2.21.1 255.255.255.0 secondary
ip address 192.3.23.1 255.255.255.0
ip pim sparse-dense-mode
ip igmp static-group 231.1.1.1
no cable arp filter request-send
no cable arp filter reply-accept
cable l3-mobility 192.0.3.1 255.255.255.0
cable l3-mobility 192.2.21.1 255.255.255.0
cable l3-mobility 192.3.23.1 255.255.255.0
cable l3-mobility 2001:DB:26:1::1/64
cable l3-mobility 2001:DB:27:1::1/96
cable dhcp-giaddr primary
cable helper-address 20.1.0.3
ipv6 address 2001:DB:26:1::1/64
ipv6 address 2001:DB:27:1::1/96
ipv6 enable
ipv6 nd reachable-time 3600000
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB:1:1:214:4FFF:FEA9:5863
end
```

Example: Configuring PXF Divert-Rate-Limit

The following example shows how to configure the PXF divert rate limit mobility counter and mobility timeslot:

```
Router# show run | in divert-limit
service divert-limit l3-mobility-counter 127
service divert-limit l3-mobility-timeslot 100
```

Additional References

The following sections provide references related to Spectrum Management and Advanced Spectrum Management for the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
CMTS Command Reference	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html Cisco Broadband Cable Command Reference Guide.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Layer 3 CPE Mobility

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

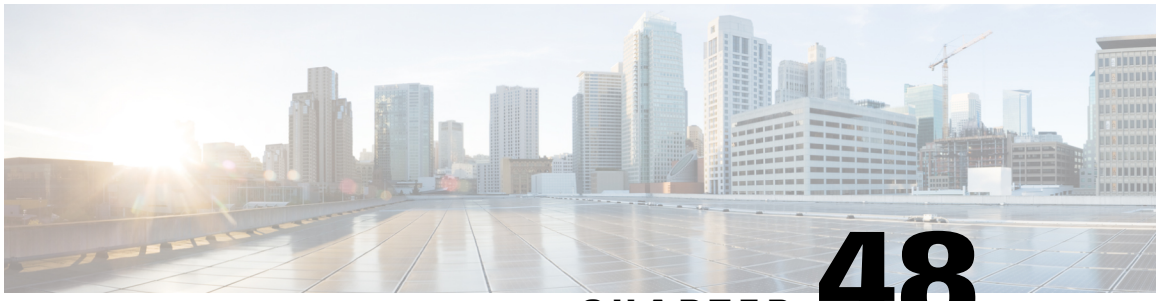
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 127: Feature Information for Layer 3 CPE Mobility

Feature Name	Releases	Feature Information
Layer 3 Mobility	12.2(33)SCH2	This feature was introduced for the Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.

PART VII

PacketCable and PacketCable Multimedia Features



CHAPTER 48

COPS Engine Operation on the Cisco CMTS Routers

Revised: February 9, 2009

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Cisco IOS Release 12.3(13a)BC introduces support for the Common Open Policy Service (COPS) engine feature on the Cisco universal broadband routers. The Cisco Cable Modem Termination System (CMTS) also supports Access control lists (ACLs) with the COPS engine.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

• Feature Information for COPS Engine Operation on the Cisco CMTS Routers , page 1293

Prerequisites for the COPS Engine on the Cisco CMTS Routers

- A compatible policy server must be connected to the network, such as the Cisco COPS QoS Policy Manager.
- Compliance with administrative policy, such as the Computer Assisted Law Enforcement Act (CALEA) or other lawful intercept (LI), is required for use of this feature on the Cisco CMTS routers.
- COPS for the Cisco CMTS routers is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Table below shows the hardware compatibility prerequisites for this feature.

Table 128: COPS Engine Operation on the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(13a)BC • PRE-2 Cisco IOS Release 12.2(33)SCA • PRE-2	Cisco IOS Release 12.3(13a)BC • Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card • Cisco uBR10-LCP2-MC28C Cable Interface Line Card • Cisco uBR10-MC5X20S/U/H Broadband Processing Engine Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.3(13a)BC • NPE-200 or later Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.3(13a)BC • Cisco uBR-MC16U/X and Cisco MC16C/S/E Cable Interface Line Cards • Cisco uBR-MC28U/X and Cisco MC28C Cable Interface Line Cards Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Restrictions for the COPS Engine on the Cisco CMTS

- Resource Reservation Protocol (RSVP) is not configured on the Cisco CMTS. COPS engine configuration on the Cisco CMTS is limited to networks in which separate RSVP and COPS Servers are configured and operational.

Information About the COPS Engine on the Cisco CMTS

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices.

COPS works in correspondence with the Resource Reservation Protocol (RSVP), which is a means for reserving network resources—primarily bandwidth—to guarantee that applications sending end-to-end across the Internet will perform at the desired speed and quality. RSVP is not configured on the Cisco CMTS, but the Cisco CMTS presumes RSVP on the network for these configurations.

Refer to the Additional References, on page 1291 for further information about COPS for RSVP.

How to Configure the COPS Engine on the Cisco CMTS

This section describes the tasks for configuring the COPS for RSVP feature on the Cisco CMTS.

To configure the COPS engine on the Cisco CMTS, perform the following tasks:

Configuring COPS TCP and DSCP Marking

This feature allows you to change the Differentiated Services Code Point (DSCP) marking for COPS messages that are transmitted or received by the Cisco router. The **cops ip dscp** command changes the default IP parameters for connections between the Cisco router and COPS servers in the cable network.

DSCP values are used in Quality of Service (QoS) configurations on a Cisco router to summarize the relationship between DSCP and IP precedence. This command allows COPS to remark the packets for either incoming or outbound connections.

The default setting is 0 for outbound connections. On default incoming connections, the COPS engine takes the DSCP value from the COPS server initiating the TCP connection.

Note This feature affects all TCP connections with all COPS servers.

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

Perform the following steps to enable optional DSCP marking for COPS messages on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cops ip dscp** [<**0-63**> | **default** | **af11-af43** | **cs1-cs7**] **Example:** `Router(config)# cops ip dscp default`	Specifies the marking for COPS messages that are transmitted by the Cisco router. The values for this command specify the markings with which COPS messages are transmitted. The following values are supported for the Cisco CMTS router: • **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)

	Command or Action	Purpose
		• **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)
Step 4	exit **Example:** `Router(config)# exit` `Router#`	Returns to privileged EXEC mode.

Configuring COPS TCP Window Size

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.

Perform the following steps to change the TCP Window size on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cops tcp window-size** *bytes* **Example:** `Router(config)# cops tcp window-size 64000`	Overrides the default TCP receive window size on the Cisco CMTS. To return the TCP window size to a default setting of 4K, use the **no** form of this command. **Note** The default COPS TCP window size is 4000 bytes. **Note** 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. **Note** This command affects all TCP connections with all COPS servers.
Step 4	**exit** **Example:** `Router(config)# exit` `Router#`	Returns to privileged EXEC mode.

Configuring Access Control List Support for COPS Engine

Cisco IOS Release 12.3(13)BC introduces support for Access Control Lists (ACLs) for COPS. Perform the following steps to configure COPS ACLs on the Cisco CMTS.

Note When using ACLs with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cops listeners access-list** { *acl-num* | *acl-name* } **Example:** `Router# cops listeners access-list 40`	Configures access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS. To remove this setting from the Cisco CMTS, us the **no** form of this command.
Step 4	**exit** **Example:** `Router(config)# exit` `Router#`	Returns to privileged EXEC mode.

What to Do Next

Access lists can be displayed by using the **show access-list** command in privileged EXEC mode.

Restricting RSVP Policy to Specific Access Control Lists

Cisco IOS Release 12.3(13)BC introduces support for Access Control Lists (ACLs) with COPS, and further supports the option of restricting the RSVP policy to specific access control lists (ACLs).

Perform the following steps to restrict the RSVP policy to specific ACLs, as already configured on the Cisco CMTS.

For ACL configuration, refer to the Configuring Access Control List Support for COPS Engine, on page 1286.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** (*slot* /*subslot* /*port* } **Example:** `Router(config)#interface cable 8/0/1` `Router(config-if)#`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip rsvp policy cops** *ACL-1 ACL-2* **servers** *iP-addr1 IP-addr2* **Example:** `Router(config-if)# ip rsvp policy cops 40 160 servers 161.44.130.164 161.44.129.2`	Tells the router to apply RSVP policy to messages that match the specified ACLs, and specifies the COPS server or servers for those sessions.
Step 5	exit **Example:** `Router(config)# exit` `Router#`	Returns to privileged EXEC mode.

Displaying and Verifying COPS Engine Configuration on the Cisco CMTS

Once COPS is enabled and configured on the Cisco CMTS, you can verify and track configuration by using one or all of the **show** commands in the following steps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show cops servers** **Example:** `Router# show cops servers`	Displays server addresses, port, state, keepalives, and policy client information.
Step 3	**show ip rsvp policy cops** **Example:** `Router# show ip rsvp policy cops`	Displays policy server addresses, ACL IDs, and client/server connection status.
Step 4	**show ip rsvp policy** **Example:** `Router# show ip rsvp policy`	Displays ACL IDs and their connection status.

Show Commands for COPS Engine Information

The following examples display three views of the COPS engine configuration on the Cisco router. These respective show commands verify the COPS engine configuration.

Displaying COPS Servers on the Network

This example displays the policy server address, state, keepalives, and policy client information:

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

Displaying COPS Policy Information on the Network

This example displays the policy server address, the ACL ID, and the client/server connection status:

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

Displaying Access Lists for COPS

This example displays the ACL ID numbers and the status for each ACL ID:

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

Debugging the COPS Engine on the Cisco CMTS

Cisco IOS Release 12.3(13a)BC and later releases support the following commands for debugging the COPS Engine on the Cisco CMTS:

Debugging COPS for PacketCable

To enable debugging processes for PacketCable with the COPS engine, use the debug packetcable cops command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug packetcable cops

no debug packetcable cops

The following example illustrates the **debug packetcable cops** command.

```
Router# debug packetcable cops
Pktcbl COPS msgs debugging is on
```

Debugging PacketCable Gate Control

To enable and display debugging processes for PacketCable gate control, use the **debug packetcable gate control** command in privileged EXEC mode. To disable this debugging, use the **no** form of this command:

debug packetcable gate control

no debug packetcable gate control

The following example illustrates gate control debugging:

```
Router# debug packetcable gate control
Pktcbl gate control msgs debugging is on
```

Debugging PacketCable Subscribers

To enable and display debugging processes for PacketCable subscribers, use the **debug packetcable subscriber** command in privileged EXEC mode. To disable this debugging, use the **no** form of this command:

debug packetcable subscriber *IP-addr*

no debug packetcable subscriber *IP-addr*

The following example illustrates the activation of the debug packetcable subscriber command for the specified IP address:

```
Router# debug packetcable subscriber 68.1.2.5
Pktcbl on the subscriber debugging is on
```

Displaying Enabled Debug Functions

To display current debugging information that includes PacketCable COPS messages on the Cisco CMTS, use the **show debug** command in privileged EXEC mode.

```
Router# show debug
PacketCable Client:
  Pktcbl COPS msgs debugging is on
PacketCable specific:
  Debugging is on for Subscriber 68.1.2.4, Mask 255.255.255.255
SLOT 6/0: Nov 19 04:57:09.219: %UBR10000-5-UNREGSIDTIMEOUT: CMTS deleted unregistered Cable
 Modem 0002.8a8c.8c1a
SLOT 6/0: Nov 19 04:57:12.279: %UBR10000-5-UNREGSIDTIMEOUT: CMTS deleted unregistered Cable
 Modem 0002.8a8c.92ae
*Nov 19 04:57:19.751: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.751: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(ndle: 0x63982B08] from COPS engine
```

COPS Engine Configuration Examples for Cable

The following sections provide COPS for RSVP configuration examples on the Cisco CMTS:

Example: COPS Server Specified

The following example specifies the COPS server and enables COPS for RSVP on the server. Both of these functions are accomplished by using the **ip rsvp policy cops** command. By implication, the default settings for all remaining COPS for RSVP commands are accepted.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy cops servers 161.44.130.168 161.44.129.6
Router(config)# exit
```

Example: COPS Server Display

The following examples display three views of the COPS for RSVP configuration on the router, which can be used to verify the COPS for RSVP configuration.

This example displays the policy server address, state, keepalives, and policy client information:

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

This example displays the policy server address, the ACL ID, and the client/server connection status:

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

This example displays the ACL ID numbers and the status for each ACL ID:

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	Cisco CMTS Cable Command Reference

Related Topic	Document Title
COPS for RSVP	• *Configuring COPS for RSVP* http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-4t/cops_rsvp.html • *COPS for RSVP* http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html

Standards

Standard	Title
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification (http://www.packetcable.com)

MIBs

MIB	MIBs Link
• No MIBs have been introduced or enhanced for support of this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
General RFC Resources	• *RFC Index Search Engine* http://www.rfc-editor.org/rfcsearch.html • *SNMP: Frequently Asked Questions About MIB RFCs* http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800c2612.shtml

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for COPS Engine Operation on the Cisco CMTS Routers

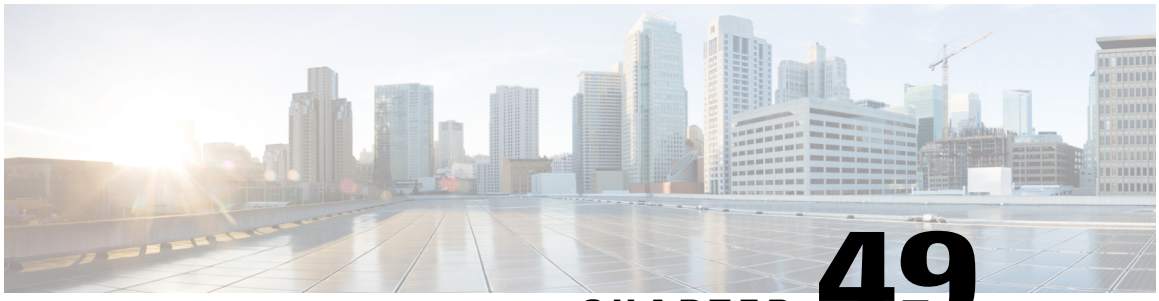
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 129: Feature Information for COPS Engine Operation on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Access Control for COPS/TCP Ports	12.3(13a)BC	Support for Common Open Policy Service (COPS) engine and Access Control Lists for COPS introduced for the Cisco uBR10012 router and Cisco uBR7246VXR router. The following commands are new or modified: • **cops ip dscp** • **cops listeners access-list** • **cops tcp window-size**
PacketCable Client Accept Timeout	12.3(21)BC	Support for the PacketCable Client Accept Timeout feature was added.

Feature Name	Releases	Feature Information
COPS Support for PacketCable	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 49

PacketCable and PacketCable Multimedia on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: January 28, 2016

Note Cisco IOS Release 12.2(33)SCA integrates support for the PacketCable and PacketCable Multimedia on the Cisco CMTS Routers feature. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure the Cisco CMTS for PacketCable and PacketCable Multimedia operations over an existing DOCSIS (1.1and later versions) network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for PacketCable Operations

This section provides information about requirements for the PacketCable feature on the Cisco CMTS routers. For information about requirements for PacketCable Multimedia on the Cisco CMTS routers, see the Prerequisites for PacketCable Multimedia Operations, on page 1317.

PacketCable Prerequisites

- To support PacketCable 1.0 and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR7246VXR broadband router must be running Cisco IOS Release 12.2(33)SCA or later.
- To support PacketCable 1.0 and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR10012 router must be running Cisco IOS Release 12.2(33)SCA or later.

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 130: PacketCable Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [84]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [85]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

84 Cisco uBR3GX60V cable interface line card is compatible only with PRE4.
85 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for PacketCable Operations

- To avoid packet drops of voice calls, the Cisco CMTS should be using the default token bucket configuration (**cable downstream rate-limit token-bucket shaping**). Packet drops are guaranteed to occur when the **shaping** option is not used (**cable downstream rate-limit token-bucket**).

- Supports only embedded multimedia terminal adapter (E-MTA) clients. Standalone MTA (S-MTA) clients are not supported.
- PacketCable operations can be configured together with HCCP N+1 redundancy, but the PacketCable states are not synchronized between the Working and Protect interfaces. If a switchover occurs, existing voice calls continue, but when the user hangs up, PacketCable event messages are not generated because the Protect interface is not aware of the previous call states. However, new voice calls can be made and proceed in the normal fashion.
- The 200,000 Hz channel width cannot be used on upstreams that support PacketCable voice calls, or on any upstreams that use Unsolicited Grant Service (UGS) or UGS with Activity Detection (UGS-AD) service flows. Using this small a channel width with voice and other UGS/UGS-AD service flows results in calls being rejected because of "DSA MULTIPLE ERRORS".

Information About PacketCable Operations

This section provides an overview and other information about PacketCable operations, the components of a PacketCable network, and how they interact with the other components of a DOCSIS cable networks.

Feature Overview

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 noncable 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.

Emergency 911 Features

Cisco IOS Release 12.2(33)SCA includes support for the following two Emergency 911 features that were introduced in Cisco IOS Release 2.3(13a)BC:

PacketCable Emergency 911 Cable Interface Line Card Prioritization

The PacketCable Emergency 911 cable interface line card prioritization feature enables cable interface line cards that are supporting an Emergency 911 call to be given automatic priority over cable interface line cards supporting non-emergency voice calls, even in the case of HCCP switchover events. In such cases, Protect HCCP line card interfaces automatically prioritize service to Emergency 911 voice calls, should Working HCCP cable interface line cards be disrupted. This feature is enabled by default, and may not be disabled with manual configuration.

Note Emergency 911 cable interface line card prioritization applies only to PacketCable voice calls.

During HCCP switchover events, cable modems recover in the following sequence:

1. Cable modems supporting Emergency 911 voice traffic
2. Cable modems supporting non-emergency voice traffic
3. Cable modems that are nearing a T4 timeout event, in which service would be disrupted
4. Remaining cable modems

To view information about Emergency 911 voice events and cable interface line card prioritization on the Cisco CMTS router, use the show hccp, show cable calls, and show hccp event-history commands in privileged EXEC mode.

PacketCable Emergency 911 Services Listing and History

Cisco IOS release 12.2(33)SCA includes enhanced informational support for PacketCable Emergency 911 calls on the Cisco CMTS router.

The enhanced informational support for PacketCable Emergency 911 calls on the Cisco CMTS router provides the following information and related history:

- active Emergency 911 calls
- recent Emergency 911 calls
- regular voice calls
- voice calls made after recent Emergency 911 calls

This feature is enabled and supported with the following configuration and show commands:

- cable high-priority-call-window
- **show cable calls**
- **show cable modem calls**

To set the call window (in minutes) during which the Cisco CMTS router maintains records of Emergency 911 calls, use the cable high-priority-call-window command in global configuration mode. To remove the call window configuration from the Cisco CMTS router, use the **no** form of this command:

The following command example configures the call window on the Cisco uBR10012 router to be 1 minute in length:

```
Router(config)# cable high-priority-call-window 1
```

PacketCable Network Components

A PacketCable network contains a number of components. Some components are the same as those that exist in a DOCSIS 1.1 network, while other components are new entities that create the end-to-end infrastructure that the PacketCable network needs to establish calls. Wherever possible, the PacketCable components and protocols build on existing protocols and infrastructures to simplify implementation and interoperability.

- Cable modem—A customer premises equipment (CPE) device that connects to a DOCSIS 1.0 or DOCSIS 1.1 cable network. All DOCSIS cable modems provide high-speed data connectivity to the Internet, while other cable modems can provide additional features, such as telephone connectivity.
- Cable Modem Termination System (CMTS)—A headend-based router that connects a DOCSIS cable network to the IP backbone network. The CMTS controls the DOCSIS 1.1 MAC layer and enforces the quality of service (QoS) limits that the cable operator guarantees to its subscribers. A typical CMTS

services between several hundred and several thousand cable modems. The Cisco uBR7246VXR and Cisco uBR10012 routers operate as the CMTS in the PacketCable network.

Note See the DOCSIS 1.1 specifications for information about cable modem and CMTS operations.

- Multimedia terminal adapter (MTA)—A CPE device that connects telephones and other end-user devices to the PacketCable network. The PacketCable specification defines two MTA types, an embedded MTA (E-MTA) and a standalone MTA (S-MTA). The E-MTA is an MTA integrated into a DOCSIS 1.1 cable modem, while the S-MTA is a separate MTA that requires a DOCSIS 1.1 cable modem to connect to the cable network.
- Call management server (CMS)—A centrally located server that provides the signaling functions that allow MTAs to establish calls over the network. The CMS uses the Network-based call signaling (NCS) protocol to provide authentication and authorization, call routing, and support for special features such as three-way calling. A PacketCable network could have multiple CMS servers, depending on its size and complexity.

Note The CMS implements several protocols on top of the Common Open Policy Service (COPS) protocol to communicate with the rest of the PacketCable network.

- Gate controller (GC)—A server that controls the establishment of gates in the PacketCable network. A gate is a logical entity in the CMTS that ensures that a service flow is authorized for the QoS features it is requesting. A separate gate controls the upstream and downstream directions of a service flow. When a call is established, the GC instructs the CMTS to create each gate and supplies the set of authorized parameters for each gate, which the CMTS uses to authorize the QoS requests that the MTA is making for the call. The GC is also responsible for coordinating the creation of the two sets of gates at each end of the call so that the call can be authorized and established.

Note A PacketCable network can contain multiple GCs, although only one server at a time is in control of any particular call. Typically, the same workstation provides both the CMS and GC servers.

- Record keeping server (RKS)—Billing server that collects the information about each call as it is made. The RKS uses the Remote Authentication Dial-In User Service (RADIUS) protocol to collect the billing data from the CMTS and other PacketCable servers. The RKS generates a call data record (CDR) for every call and forwards that information to the appropriate application server at the service provider's data processing center for further processing.

Dynamic Quality of Service

A key feature of a PacketCable network is a dynamic quality of service (DQoS) capability that is similar to the dynamic services provided by DOCSIS 1.1. However, DOCSIS 1.1 DQoS authorizes and provisions services only in the cable network and does not reserve the resources needed to propagate a call from one endpoint to another across the network.

The PacketCable DQoS extends the DOCSIS 1.1 services across the entire network, so that resources can be dynamically authorized and provisioned from one endpoint to another. This prevents possible theft-of-service attacks and guarantees customers the services they are authorized to use.

Note PacketCable 1.0 requires that DOCSIS 1.1 be used for resource reservation within the cable network for E-MTA clients.

Two-Stage Resource Reservation Process

The PacketCable DQoS model uses a two-stage resource reservation process, in which resources are first reserved and then committed. This allows a bidirectional reservation process that ensures that resources are available at both endpoints of the connection before actually placing the call.

When an MTA makes a call request, the local CMTS communicates with the gate controller to authorize the call's resources. After the resources are authorized, the CMTS reserves the local resources while it negotiates with the remote end for the resources that are required at that end.

Note The CMTS uses DOCSIS 1.1 Dynamic Service Addition (DSA) messages to reserve the resources, and then uses Dynamic Service Change (DSC) messages to commit the resources.

When all required resources are available, the local CMTS and remote CMTS both commit the resources, allowing traffic to flow. Usage accounting and billing do not begin until the remote MTA picks up and the call is actually in progress.

The DQoS model ensures that both endpoints of a call, as well as the backbone network, have reserved the same bandwidth, and that the bandwidth is reserved only while the call is in progress. When a call terminates, all portions of the network can release the call's resources and make them available for other users.

Making a Call Using DQoS

DOCSIS 1.1 networks use service flows to implement different QoS policies, but service flows exist only within the cable network. To control the service flows and to extend them across the entire network, a PacketCable network creates and maintains "gates."

A gate is a logical entity created on the CMTS at each side of a connection that authorizes and establishes a particular DQoS traffic flow. The CMTS communicates with the gate controller to coordinate the creation of matching gates at each side of the connection.

Gates are unidirectional, so separate gates are required for the downstream and upstream traffic flows. The same gate ID, however, is usually used for the downstream and upstream gates for a call. Each CMTS maintains its own set of gates, so a bidirectional traffic flow requires four gates to be created, two gates on the local CMTS and two gates on the remote CMTS.

For a typical call, gates progress through the following stages to create a DQoS traffic flow:

1. The local MTA makes a call request, and the gate controller sends a Gate-Allocation command to the CMTS, which creates a gate in response and puts it into the Allocated state.
2. The call management server, which might be the same server as the gate controller, parses the call request to translate the destination phone number into the appropriate destination gateway.
3. The gate controller verifies that the MTA making the call request is authorized for the required resources and sends a Gate-Set command to the CMTS, which puts the gate into the Authorized state.

4. The CMTS on each side of the connection reserves the local resources needed for the call, putting the gate into the Reserved state.
5. As the remote CMTS and local CMTS perform gate coordination, their respective gates get put into the Local_Committed and Remote_Committed states.
6. When both sides have reserved all required resources, each CMTS puts its gates into the Committed state, allowing traffic to flow.

Dynamic Service Transaction ID Support

DOCSIS 2.0 mandates unique Transaction IDs (TAIDs) across transactions. The TAIDs must be unique and not incremented. The TAIDs are assigned by the senders and sometimes the TAID timeout is mismatched between senders and receivers. This affects the uniqueness of the TAID.

A TAID can be reused when the sender finishes a transaction. Similarly, DOCSIS allows the receiver to identify a transaction by TAID without the SFID. Problems arise in DSD transaction and DSA/DSC interrupted transactions, when these two requirements are combined.

The uniqueness of TAID must be ensured to resolve the interoperability issue. This is done by making the CMTS wait until T10 to reuse the same TAID. A new TAID allocation algorithm is used to fulfill this requirement.

It creates a TAID pool to replace the existing 16-bit counter. This TAID pool is monitored by timers to track the TAID expiration. A flag is assigned to each TAID in the pool to indicate its availability. When new TAID is requested, the dynamic service process checks the availability of the TAID. If the TAID is available, it is allocated to the new service flow, else the request is rejected.

Once the TAID is allocated, the timer starts with T10 expiration time and the TAID flag is set to FALSE to indicate the unavailability of TAID. The dynamic service process keeps track of the timer. When the time expires, the timer stops and the flag is set to TRUE to indicate the availability of TAID.

The TAID pool is allocated and initialized at the process initialization. All timers associated with the TAIDs are added as leaf timers to the process' parent timer.

PacketCable Subscriber ID Support

The PacketCable Subscriber ID feature adds a subscriber ID to all Gate Control messages and enhances error codes returned from the Cisco CMTS router.

Previously, the Gate ID was unique only to individual CMTS systems, with the CMTS proxying all CMS Gate Control messaging through a central device, which manages the CMTS connections on behalf of the CMS. The CMS had a single Common Open Policy Service (COPS) association to the proxy device. Therefore, the Gate IDs could be duplicated when using multiple CMTS systems.

A subscriber ID is added to each Gate Control message to disambiguate the Gate IDs between the CMS and proxy device. The subscriber ID parameter is added to the following COPS messages:

- GATE-INFO
- GATE-DELETE
- GATE-OPEN
- GATE-CLOSE

The subscriber ID is available at the CMS and is used in the Gate-Set messages. Additionally, the error codes returned from CMTS or its proxy are enhanced to include more specific information about gate operation failures.

To enable this feature, use the **packetcable gate send-subscriberID** command in global configuration mode.

Note The PacketCable Subscriber ID feature is not supported in Cisco IOS Release 12.2(33)SCA. However, it is supported beginning in Cisco IOS Release 12.2(33)SCB.

Benefits

The PacketCable feature offers the following benefits to service providers and their customers:

Integrated Services on a Cable Network

PacketCable allows cable operators the ability to offer multimedia, real-time services, in addition to data connectivity, across their entire network. These services could include basic telephony with lifeline support, as well as telephony that offers competitive extended calling services. Operators can deploy new services while heavily leveraging their existing network infrastructures.

The widespread use of IP as the standard transport mechanism for data networks today is enabling many advanced Internet applications such as multimedia e-mail, real-time chat, streaming media (including music and video), and videoconferencing. The PacketCable initiative provides the network architecture for a cable operator to deliver these services quickly and economically.

Standardized Provisioning

PacketCable provides a standardized, efficient method to provision IP services for individual subscribers, because PacketCable specifications define a uniform, open, and interoperable network. Cable operators are assured of standardized provisioning and the associated lower costs of deployment.

Interoperability

Customer premises equipment (CPE) devices account for a major portion of the capital expense in deploying a VoIP solution at a cable plant. The PacketCable specifications ensure that vendors will build MTA clients that support the voice and other services that cable operators plan to deploy. Because these CPE devices are based on existing DOCSIS-compliant cable modems, time and cost of development is minimized.

Interoperability with the other components of the PacketCable network is also guaranteed because of the standards-based approach to the specifications. Any PacketCable-certified component will be able to interoperate within a network that conforms to the PacketCable standards.

Secure Architecture

Because PacketCable is built upon the security features available in DOCSIS 1.1, cable operators will be assured of networks that are secure from end to end, with a high standard of security that prevents the most common theft-of-service attacks. The comprehensive, standards-based PacketCable specifications are designed to create a network that is as secure as the public switched telephone network (PSTN).

CALEA Support

The PacketCable architecture was designed to accommodate the 1994 Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers to assist law-enforcement agencies in conducting court-ordered electronic surveillance. PacketCable networks will be able to provide the two types of information that a carrier must provide, depending on the type of court order:

- Call-identifying information—The carrier must provide the call-identifying information for calls to or from an intercept target. For telephone calls, this information includes the phone numbers called by the target or calling the target.
- Call content—The carrier must provide the content of calls to or from an intercept target. For telephone calls, this real-time content is the voice conversation.

How to Configure PacketCable Operations

This section contains the following tasks to configure the PacketCable feature. Each task is required unless otherwise identified as optional.

Enabling PacketCable Operation

To enable PacketCable operation, use the following commands beginning in user EXEC mode. This is a required procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**packetcable** **Example:** `Router(config)# packetcable`	Enables PacketCable operation on all cable interfaces.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Disabling PacketCable Operation

To disable PacketCable operation, use the following commands beginning in user EXEC mode. This procedure is required only when you no longer want the Cisco CMTS to support PacketCable signaling.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no packetcable** **Example:** `Router(config)# no packetcable`	Disables PacketCable operation on all cable interfaces.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring PacketCable Operation

To configure the different parameters that affect PacketCable operations, use the following commands beginning in user EXEC mode. All of these procedures are optional, because each parameter is set to a default that is appropriate for typical PacketCable operations.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**packetcable element-id** *n* **Example:** `Router(config)# packetcable element-id 23`	Configures the Event Message Element ID for the Cisco CMTS. If you do not manually configure the Element ID, the CMTS defaults to a random value between 0 and 99,999 when PacketCable operations are enabled.
Step 4	**packetcable gate maxcount** *n* **Example:** `Router(config)# packetcable gate maxcount 524288`	Sets the maximum number of gate IDs to be allocated in the gate database on the Cisco CMTS.
Step 5	**packetcable timer T0** *timer-value* **Example:** `Router(config)# packetcable timer T0 40000`	Sets the T0 timer in milliseconds.
Step 6	**packetcable timer T1** *timer-value* **Example:** `Router(config)# packetcable timer T1 300000`	Sets the T1 timer in milliseconds.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Enabling Both PacketCable and Non-PacketCable UGS Service Flows

By default, when PacketCable operations are enabled using the **packetcable** command, cable modems must follow the PacketCable protocol when requesting Unsolicited Grant Service (UGS) service flows. This prevents DOCSIS cable modems that do not support PacketCable operations from using DOCSIS-style UGS service flows.

If you have a mixed network that contains both PacketCable and non-PacketCable DOCSIS CMs, you can use the **packetcable authorize vanilla-docsis-mta** command to enable both types of UGS service flows. This is an optional procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**packetcable** **Example:** `Router(config)# packetcable`	Enables PacketCable operations.
Step 4	**packetcable authorize vanilla-docsis-mta** **Example:** `Router(config)# packetcable authorize vanilla-docsis-mta`	Enables the use of DOCSIS-style UGS service flow requests.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Tip Use the **show packetcable global** command to display whether non-PacketCable UGS service flows have been enabled.

Enabling PacketCable Subscriber ID Support

To include subscriber identification in GATE-OPEN and GATE-CLOSE Gate Control messages, use the **packetcable gate send-subscriberID** command in global configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**packetcable** **Example:** `Router(config)# packetcable`	Enables PacketCable operations.
Step 4	**packetcable gate send-subscribeID** **Example:** `Router(config)# packetcable gate send-subscriberID`	Enables the use of gate control subscriber identification information.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring RADIUS Accounting for RKS Servers

To enable the Cisco CMTS router to communicate with the Record Keeping Servers (RKS servers) using the RADIUS protocol, use the following commands. This is a required procedure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius packetcable`	Creates a group of RADIUS servers for authentication and enters RADIUS group configuration mode. The value of *group-name* is a unique, arbitrary string that identifies this group.
Step 5	**server** {*hostname* | *ip-address*} [**auth-port** *udp-port*] [**acct-port** *udp-port*] **Example:** `Router(config-sg-radius)# server radius-server1`	Specifies the host name or IP address for the RADIUS server that is providing the RKS services. **Note** Repeat this command as needed to enter multiple RADIUS servers. The Cisco CMTS uses the servers in the order given with this command.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits RADIUS group configuration mode.
Step 7	**aaa accounting network default start-stop group radius group** *group-name* **Example:** `Router(config)# aaa accounting network default start-stop group radius group packetcable`	Enables AAA services using the group of RADIUS servers that are defined in the previously created group. The *group-name* parameter should be the same name specified in Step 4 .
Step 8	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] **key 0000000000000000** **Example:** `Router(config)# radius-server host radius-server1 key 0000000000000000`	Specifies a RADIUS host. Use the same values for *hostname* or *ip-address* as for one of the servers specified in Step 5 . If you also specified the **auth-port** or **acct-port** values in Step 5 , you must also specify those here, as well. The **key** value is required and must be 16 ASCII zeros, as shown. **Note** Repeat this command for each RADIUS server entered in Step 5 .

	Command or Action	Purpose
Step 9	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Configures the Cisco CMTS to recognize and use accounting-related vendor-specific attributes (VSA).
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Troubleshooting Tips

If the connection between a PacketCable CMS and the Cisco CMTS router is not completely established, and the PacketCable CMS does not correctly terminate the session by sending a TCP FIN message, the connection shows a COPS server in the output of the **show cops server** command.

PacketCable Client Accept Timeout

The PacketCable Client Accept Timeout feature supports COPS for PacketCable on the Cisco CMTS router. This feature also allows you to set timeout values for COPS Telnet connections on the Cisco CMTS router, and for clearing COPS Telnet sessions.

Telnet errors on the network or Cisco CMTS router might cause incomplete COPS sessions to be created. In order to address this issue, the timeout timer enables clearing and cleaning of allocated resources for the stale COPS Telnet sessions on the Cisco CMTS router.

The timeout timer applies to each COPS Telnet connection on the Cisco CMTS router. When this timeout setting expires, it terminates the Telnet session and clears supporting resources on the Cisco CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**packetcable timer** {**T0** *timer-value* | **T1** *timer-value* | **multimedia T1** *timer-value*} **Example:** `Router(config)# packetcable timer T0 300000` **Example:** `Router(config)# packetcable timer T1 400000` **Example:** `Router(config)# packetcable timer multimedia T1 400000`	Sets the PacketCable timer value.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

If the connection between a PacketCable CMS and the Cisco CMTS router is not completely established, and the PacketCable CMS does not correctly terminate the session by sending a TCP FIN message, the connection shows a COPS server in the output of the **show cops server** command.

Configuration Examples for PacketCable

This section provides a PacketCable configuration example.

Example: Typical PacketCable Configuration

This section provides a typical configuration for a Cisco CMTS router that has been configured for PacketCable operations, using default parameters. To use this configuration, you must change the IP addresses for the RADIUS and RKS servers to match the addresses for the servers in your network.

```
!
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
service tcp-small-servers max-servers no-limit
!
hostname Router
```

```
!
no logging rate-limit
aaa new-model
!
!
aaa group server radius a
 server 10.9.62.12 auth-port 1813 acct-port 1812
 server 10.9.62.13 auth-port 1813 acct-port 1812
!
aaa accounting network default start-stop group radius group a
aaa session-id common
enable password <delete>
!
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 5 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 5 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 short 6 78 7 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 5 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16
cable qos profile 5 max-burst 1200
cable qos profile 5 max-downstream 2000
cable qos profile 5 max-upstream 128
cable qos profile 5 priority 5
cable qos profile 5 privacy
cable qos profile 7 guaranteed-upstream 87
cable qos profile 7 max-upstream 87
cable qos profile 7 privacy
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable qos permission enforce 5
cable time-server
no cable privacy accept-self-signed-certificate
ip subnet-zero
!
!
no ip domain-lookup
ip domain-name cisco.com
ip host tftp 10.8.8.8
ip host cnr 10.9.62.17
!
packetcable
packetcable element-id 12456
!
!
!
interface Tunnel0
 ip address 10.55.66.3 255.255.255.0
 load-interval 30
 tunnel source FastEthernet1/0
 tunnel destination 172.27.184.69
!
interface Tunnel10
 ip address 10.0.1.1 255.255.0.0
!
interface FastEthernet0/0
 ip address 10.9.60.10 255.255.0.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface FastEthernet1/0
 ip address 172.22.79.44 255.255.254.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface Cable3/0
 ip address 10.3.1.33 255.255.255.0 secondary
```

```
 ip address 10.4.1.1 255.255.255.0 secondary
 ip address 10.4.1.33 255.255.255.0 secondary
 ip address 10.3.1.1 255.255.255.0
 ip helper-address 10.9.62.17
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 55500000
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 12000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 data-backoff automatic
 cable upstream 1 modulation-profile 2
 cable upstream 1 shutdown
 cable upstream 2 frequency 16000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 data-backoff automatic
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 20000000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 data-backoff automatic
 cable upstream 3 modulation-profile 2
 no cable upstream 3 shutdown
 cable upstream 4 frequency 24000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000
 cable upstream 4 data-backoff automatic
 no cable upstream 4 shutdown
 cable upstream 5 frequency 28000000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 3200000
 cable upstream 5 data-backoff automatic
 cable upstream 5 modulation-profile 2
 no cable upstream 5 shutdown
 cable dhcp-giaddr policy
!
router eigrp 48849
 network 1.0.0.0
 network 10.0.0.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 10.9.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.78.1
ip route 10.8.0.0 255.255.0.0 10.9.0.1
ip route 192.168.80.0 255.255.255.0 Tunnel0
ip route 192.168.80.0 255.255.255.0 172.27.184.69
ip route 10.255.254.254 255.255.255.255 10.9.0.1
no ip http server
ip pim bidir-enable
!
!
cdp run
!
!
radius-server host 10.9.62.12 auth-port 1813 acct-port 1812 key 0000000000000000
radius-server retransmit 3
radius-server vsa send accounting
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 session-timeout 33
```

```
 exec-timeout 0 0
 password <deleted>
!
ntp clock-period 17179976
ntp server 1.9.35.8
end
```

Verifying PacketCable Operations

To verify and maintain information about PacketCable operations, use one or more of the following commands:

- **show packetcable global**
- **show packetcable gate**
- **show packetcable gate ipv6**
- **show packetcable gate dqos**
- **show packetcable gate counter commit**

To verify the PacketCable configuration, values for the Element ID, maximum number of gates, and the different CMTS-based DQoS timers, use the **show packetcable global** command in privileged EXEC mode.

```
Router# show packetcable global
Packet Cable Global configuration:
Enabled   : Yes
Element-ID: 12456
Max Gates : 1048576
Allow non-PacketCable UGS
Default Timer value -
  T0      : 30000 msec
  T1      : 300000 msec
```

To verify information about one or more gates in the gate database, use the **show packetcable gate** command as shown in the following example:

```
Router# show packetcable gate summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
13582      Ca8/1/0      3.18.1.4       20.5.0.254     RECOVERY  MM    74
29962      Ca8/1/0      3.18.1.5       20.5.0.254     RECOVERY  MM    73
46354      Ca8/1/0      ------         20.5.0.254     RECOVERY  MM    72
62738      Ca8/1/0      ------         20.5.0.254     RECOVERY  MM             69
Total number of  gates = 4
Total Gates committed(since bootup or clear counter) = 8
```

To verify information about one or more PacketCable gates associated with IPv6 subscriber IDs in the gate database, use the **show packetcable gate ipv6** command as shown in the following example:

```
Router# show packetcable gate ipv6 summary
GateID     i/f                  SubscriberID                State   SFID(us) SFID(ds)
13582      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    74
29962      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    73
46354      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    72
62738      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT             69

Total number of  gates = 4
Total Gates committed(since bootup or clear counter) = 8
```

To verify information about one or more PacketCable gates associated with IPv4 subscriber IDs in the gate database, use the **show packetcable gate dqos** command as shown in the following example:

```
Router# show packetcable gate dqos summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
13576      Ca8/1/0      40.1.43.60     10.74.58.5     COMMIT    DQoS  527      528
```

```
29956      Ca8/1/0      40.1.43.56     10.74.58.5     COMMIT    DQoS  525      526
Total number of DQOS gates = 2
Total Gates committed(since bootup or clear counter) = 346
```

To verify the total number of gates that the Cisco CMTS router has moved to the Committed state since the router was last reset, or since the counter was last cleared, use the show packetcable gate counter commit command as shown in the following example:

```
Router# show packetcable gate counter commit
Total Gates committed (since bootup or clear counter) = 132
```

Verifying Emergency 911 Calls

This section provides a few examples to illustrate how you can use the show cable calls and show cable modem calls commands to verify different scenarios associated with Emergency 911 calls.

The following example displays Emergency 911 calls made on the Cable8/1/1 interface on the Cisco CMTS router during the window set for high priority calls:

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0  0                 0               0                 0
Cable5/0/1  0                 0               0                 0
Cable5/1/0  0                 0               0                 0
Cable5/1/1  0                 0               0                 0
Cable5/1/2  0                 0               0                 0
Cable5/1/3  0                 0               0                 0
Cable5/1/4  0                 0               0                 0
Cable6/0/0  0                 0               0                 0
Cable6/0/1  0                 0               0                 0
Cable7/0/0  0                 0               0                 0
Cable7/0/1  0                 0               0                 0
Cable8/1/0  0                 0               0                 0
Cable8/1/1  1                 1               0                 0
Cable8/1/2  0                 0               0                 0
Cable8/1/3  0                 0               0                 0
Cable8/1/4  0                 0               0                 0
Total       1                 1               0                 0
```

The following example displays the change on the Cisco CMTS router when this Emergency 911 calls ends:

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0  0                 0               0                 0
Cable5/0/1  0                 0               0                 0
Cable5/1/0  0                 0               0                 0
Cable5/1/1  0                 0               0                 0
Cable5/1/2  0                 0               0                 0
Cable5/1/3  0                 0               0                 0
Cable5/1/4  0                 0               0                 0
Cable6/0/0  0                 0               0                 0
Cable6/0/1  0                 0               0                 0
Cable7/0/0  0                 0               0                 0
Cable7/0/1  0                 0               0                 0
Cable8/1/0  0                 0               0                 0
Cable8/1/1  0                 0               0                 1
Cable8/1/2  0                 0               0                 0
Cable8/1/3  0                 0               0                 0
Cable8/1/4  0                 0               0                 0
Total       0                 0               0                 1
```

The following example displays information that is available when making a voice call from the same MTA to another MTA on the same interface:

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0  0                 0               0                 0
```

```
Cable5/0/1  0                0               0                0
Cable5/1/0  0                0               0                0
Cable5/1/1  0                0               0                0
Cable5/1/2  0                0               0                0
Cable5/1/3  0                0               0                0
Cable5/1/4  0                0               0                0
Cable6/0/0  0                0               0                0
Cable6/0/1  0                0               0                0
Cable7/0/0  0                0               0                0
Cable7/0/1  0                0               0                0
Cable8/1/0  0                0               0                0
Cable8/1/1  0                2               1                1
Cable8/1/2  0                0               0                0
Cable8/1/3  0                0               0                0
Cable8/1/4  0                0               0                0
Total       0                2               1                1
```

The following example displays information that is available when a voice call from the same MTA to another MTA on the same interface ends:

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0  0                 0               0                 0
Cable5/0/1  0                 0               0                 0
Cable5/1/0  0                 0               0                 0
Cable5/1/1  0                 0               0                 0
Cable5/1/2  0                 0               0                 0
Cable5/1/3  0                 0               0                 0
Cable5/1/4  0                 0               0                 0
Cable6/0/0  0                 0               0                 0
Cable6/0/1  0                 0               0                 0
Cable7/0/0  0                 0               0                 0
Cable7/0/1  0                 0               0                 0
Cable8/1/0  0                 0               0                 0
Cable8/1/1  0                 0               0                 1
Cable8/1/2  0                 0               0                 0
Cable8/1/3  0                 0               0                 0
Cable8/1/4  0                 0               0                 0
Total       0                 0               0                 1
```

The following examples display the show cable modem calls command output on the Cisco CMTS router over a period of time, with changing call status information. The call information disappears when a call ends.

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                 0:39
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
```

The following example displays a new Emergency 911 call on the Cisco CMTS router:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    HV                1:30
```

The following example displays the end of the Emergency 911 call on the Cisco CMTS router:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                   0:3
```

The following example displays a non-emergency voice call on the Cisco CMTS router from the same MTA:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.ca36.f97d 10.10.155.25    C8/1/1/U0 5     V                     -
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    RV                  0:30
```

The following example displays the end of the non-emergency voice call on the Cisco CMTS router:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                   0:36
```

Prerequisites for PacketCable Multimedia Operations

This section provides information about requirements for the PacketCable Multimedia feature on the Cisco CMTS routers. For information about requirements for the PacketCable feature on the Cisco CMTS routers, see the Prerequisites for PacketCable Operations, on page 1296.

Cisco uBR7225VXR Router

Support for the Cisco uBR7225VXR router was introduced in Cisco IOS Release 12.2(33)SCA.

Cisco uBR7246VXR Router

- To support PacketCable Multimedia and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR7246VXR broadband router must be running Cisco IOS Release 12.2(33)SCA and later.

Cisco uBR10012 Router

- To support PacketCable Multimedia and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR10012 router must be running Cisco IOS Release 12.2(33)SCA and later.

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 131: PacketCable Multimedia Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [86]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [87]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

86 Cisco uBR3GX60V cable interface line card is compatible only with PRE4.

87 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for PacketCable Multimedia Operations

The PacketCable Multimedia feature supports only the unicast gate-based PCMM configuration in Cisco IOS Releases earlier than Cisco IOS Release 12.2(33)SCE.

Information About PacketCable Multimedia Operations

The PacketCable Multimedia (PCMM) feature is a powerful implementation of the CableLabs® standards for PacketCable Multimedia. PCMM provides enhanced QoS for multimedia applications, voice, and bandwidth-intensive services over a DOCSIS (DOCSIS 1.1 and later versions) network.

The Cisco CMTS router supports DOCSIS QoS for SIP-based telephones and SIP video phones, Bandwidth-on-Demand applications, and network-based gaming applications, all of which place extensive bandwidth demands on the network.

This section provides information about the following aspects of PacketCable Multimedia for the Cisco CMTS router, emphasizing PCMM components that are configured with the Cisco IOS command-line interface later in this document:

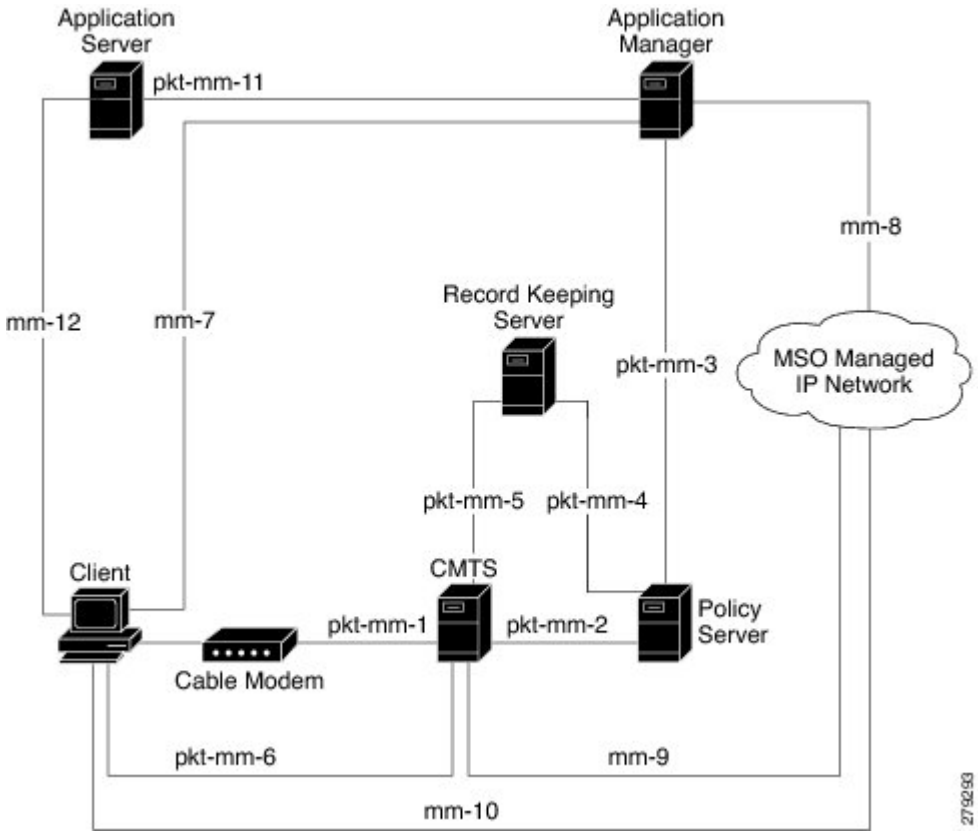
PCMM Overview

The following network components are required to support the PCMM feature:

- Application Server—Responsible for relaying client requests to the Application Manager.
- Application Manager—Responsible for application or session-level state and for applying session control domain (SCD) policy.
- Policy Server—Responsible for applying the RCD policy and for managing relationships between the Application Manager and a Cisco CMTS router.
- Cisco CMTS router—Responsible for performing admission control and managing network resources through DOCSIS service flows.

Figure below provides an architectural overview of the PCMM functionality:

Figure 30: PCMM Architectural Overview



PCMM Enhancements over PacketCable 1.x

PacketCable Multimedia is a service delivery framework that leverages and uses as much of existing PacketCable 1.x deployments and functionality as possible. Furthermore, PCMM offers powerful enhancements to the VoIP service delivery framework with straightforward CLI implementation. The key enhancements that the PCMM provides are:

- Time and volume based network resource authorizations are based on DOCSIS 1.1 Quality of Service (QoS) mechanisms.
- Event-based network resource auditing and management functions.
- Secure infrastructure that protects all interfaces at appropriate levels.
- Preauthorized model from PacketCable 1.x, where the PCMM gate installation and management is supplemented with service flow creation, modification and deletion functions. Together, these provide a secure, network-based QoS.

PCMM and High Availability Features on the Cisco CMTS Router

In Cisco IOS Release 12.2(33)SCA and later, High Availability on the Cisco CMTS router only accommodates synchronization of service flows created for the PCMM applications. This means that the PCCM gate configuration will be recreated in the standby line card in the event of a PRE or line card switchover.

PCMM Gates

PCMM Gate Overview and PCMM Dynamic Quality of Service

A PacketCable 1.x gate defines QoS parameters and policy-based authorization for subscribers, and a specific envelope of network resources. A PacketCable 1.x gate also maintains classifiers for originating and terminating IP addresses and ports.

Before Cisco IOS Release 12.2(33)SCE, the subscriber ID was used to identify only the IPv4 address of either the cable modem or the client CPE. The PCMM feature includes support for IPv6 addresses in Cisco IOS Release 12.2(33)SCE and later. This means that the subscriber ID can identify both IPv4 and IPv6 addresses.

PacketCable 1.x defines a preauthorization model. The PacketCable gates are created and installed at the Cisco CMTS router prior to network resource reservation or activation requests. This process, termed gate control, is managed through a COPS-based policy interface on the Cisco CMTS router.

In PCMM, this COPS-based interface is enhanced for QoS life-cycle management. PCMM gates maintain service flow creation, modification and deletion functions to provide for network-based QoS. Multiple PCMM gates and service flow policies can be maintained on the Cisco CMTS router at a given time, and these PCMM gates are fully interoperable with PacketCable 1.x gates.

When a cable modem subscriber requests bandwidth for a network-intensive application, the network Policy Server sends a Gate-Set message to the Cisco CMTS router. This message contains QoS, service flow, and billing information for this subscriber. This gate profile information is maintained on the Cisco CMTS router, to include PCMM gate states and PCMM state transitions.

The Cisco CMTS router initiates service flows with cable modems, and optimizes DOCSIS resource availability on the Cisco CMTS router for bandwidth-intensive service flows characteristic to PCMM.

Restrictions

On some upstream paths, best effort service flows are configured on some modems with Committed Information Rate (CIR). When a number of bandwidth requests are queued in the modems, only a few requests are sent to the CMTS. This occurs due to congestion of sending requests caused by higher number of service flows, greater traffic and small size of packets. Therefore, only a few best effort service flow requests are satisfied by the CMTS.

PCMM Persistent Gate

Cisco IOS Release 12.2(33)SCA supports the Persistent Gate feature for PacketCable Multimedia. Persistent Gate is a feature by which PCMM gate information is maintained for cable modems that go offline. This gate information is quickly enabled after a cable modem returns online. When a cable modem returns online, the Cisco CMTS router scans PCMM gates previously stored, and initiates service to the cable modem according to the respective PCMM gate. This re-enabled service maintains traffic support profiles for that gate, and allocates DOCSIS resources based on the new online subscriber.

The Cisco CMTS router maintains the PC and PCMM gate databases separately and independently. Information for either is available with multiple **show** commands.

PCMM Interfaces

PCMM optimizes the IPC handshake between the cable interface line card and the Network Processing Engine (NPE) for the Cisco uBR7246VXR router, or the Route Processor (RP) for the Cisco uBR10012 router. Additional PCMM interface changes from PacketCable 1.x include the handling for COPS interface and distributed cable interface line cards.

PCMM to COPS Interface

PCMM differs from PacketCable 1.x in handling COPS sessions. The COPS sessions on PCMM use TCP port number 3918 by default. Whereas, PacketCable uses the DQoS specification for TCP port requirements and COPS sessions.

When the PCMM module initializes for the first time, a PCMM registry is added to the cable interface line card and the route processor. The PCMM module also registers the PCMM COPS client with the COPS layer on the Cisco CMTS router.

PCMM and Distributed Cable Interface Line Cards

As with PacketCable 1.x, PCMM uses IPC messages for voice support. When PCMM gates are created on the Network Processing Engine (NPE) or route processor (RP), the PCMM gate parameters are sent to cable interface line cards. IPC maintains all communication between the NPE or RP, and the cable interface line cards.

Event messaging is used with PCMM to support billing information based on Gate-Set messages. Event messaging for distributed cable interface line cards originates from the line cards, based on the success of DSX operation.

The PCMM module also registers the PCMM COPS client with the COPS layer.

PCMM Unicast and Multicast

The PacketCable Multimedia feature supports only the unicast gate-based PCMM configuration in Cisco IOS Releases earlier than Cisco IOS Release 12.2(33)SCE. In unicast transmission, content is sent to a unique user.

Support for the PCMM multicast feature was introduced in Cisco IOS Release 12.2(33)SCE. In multicast transmission, content is sent to multiple users simultaneously.

PCMM Multicast Session Range

Beginning with Cisco IOS Release 12.2(33)SCE, you can configure a PCMM multicast session range by specifying IPv4 IP addresses and a mask for a PCMM multicast group. The PCMM multicast session range enables the Cisco CMTS router to accept Gate-Set messages from the PCMM Policy Server. If a PCMM multicast session range is configured, the Cisco CMTS router does not allow you to create multicast sessions using other sources such as Internet Group Management Protocol (IGMP) and DOCSIS Set-Top Gateway (DSG).

PCMM Multicast

Beginning with Cisco IOS Release 12.2(33)SCJ, you can enable PCMM multicast by using **packetcable multimedia** command. Now both PCMM multicast and mVPN feature can work simultaneously, except for the NextGen mVPN.

The following restrictions are applicable to the PCMM Multicast feature:

- PCMM multicast can not work in VRF.
- Encrypted PCMM multicasts Service Flows are not supported.
- The number of unique GCs, GQCs and Service-Class definitions is restricted to 512.
- After switchover, traffic forwarding can take up to 10 secs to resume.
- Locally configured GCs and GQCs on the interface will not be applicable to PCMM flows, even if they match the PCMM multicast IP address range.
- IPv6 based classifiers are not supported.
- Non-MDF capable CM will not be supported.

PCMM IPv6 Voice

Starting with Cisco IOS Release 12.2(33)SCJ, the Cisco CMTS routers support the PCMM IPv6 Voice feature. As DOCSIS 3.0 has introduced new requirements and features to be used in Cable network, PCMM I04 specification has also incorporated a list of ECN to take advantage these new DOCSIS features, and a few other enhancements. IPv6 Subscriber and Classifier ECN added new objects to support:

- IPv6 subscriber ID object for PCMM session triggering by IPv6 subscriber.
- IPv6 classifier for both upstream and downstream service flow.

How to Configure PCMM Operations

The following tasks describe how to enable PCMM operations and configure its related features on the Cisco CMTS router:

Enabling PCMM Operations on the Cisco CMTS Router

To enable PCMM operations on the Cisco CMTS router:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**packetcable multimedia** **Example:** `Router(config)# packetcable multimedia`	Enables and displays PCMM processing on the Cisco CMTS router. This command enables the Cisco CMTS router to start or stop responding to PCMM COPS messages received from the PCMM Policy Server.
Step 4	**packetcable authorize vanilla-docsis-mta** **Example:** `Router(config)# packetcable authorize vanilla-docsis-mta`	Allows non-DQoS MTAs to send DOCSIS DSX messages.
Step 5	**packetcable gate maxcount** *n* **Example:** `Router(config)# packetcable gate maxcount 890`	Sets the maximum number of PCMM gates in the gate database.
Step 6	**packetcable timer multimedia T1** *timer-value* **Example:** `Router(config)# packetcable timer multimedia T1 300000`	Sets the timeout value for T1 timer used in PCMM gate processing.
Step 7	**clear packetcable gate counter commit [dqos | multimedia]** **Example:** `Router(config)# clear packetcable gate counter commit multimedia`	(Optional) Clears the specified PCMM gate counter.
Step 8	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring a PCMM Multicast Session Range

A PCMM multicast session range enables the Cisco CMTS router to use a range of IP addresses for a PCMM multicast group.

Before You Begin

Ensure that PCMM is configured using the **packetcable multimedia command.**

Note

- You can configure only one PCMM multicast group on the Cisco CMTS router. You can configure a maximum of ten multicast sessions for a single multicast group.
- The PCMM multicast feature is supported only with the cable modems that are capable of Multicast DSID-based Forwarding (MDF).

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast source pcmm** **Example:** `Router(config)# cable multicast source pcmm`	Enables PCMM-based multicast service on the Cisco CMTS router and enters multicast session range configuration mode.
Step 4	**session-range** *ip-addressip-mask* **Example:** `Router(config)# session-range 229.0.0.0 255.0.0.0`	Configures a session range for the PCMM multicast group.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuration Examples for PacketCable Multimedia

The following sections provide configuration examples for PCMM operations on the Cisco CMTS router:

Example: Enabling PCMM Operations on the Cisco CMTS Router

```
Router# configure terminal
Router(config)# packetcable multimedia
Router(config)# packetcable authorize vanilla-docsis-mta
Router(config)# packetcable gate maxcount 890
Router(config)# packetcable timer multimedia 30000
```

Example: Enabling a Multicast Session Range on the Cisco CMTS Router

```
Router# configure terminal
Router(config)# cable multicast source pcmm
Router(config)# session-range 229.0.0.0 255.0.0.0
```

Verifying PCMM Operations

Use the following **show** commands to verify PCMM operations:

- **show packetcable gate multimedia**
- **show cable multicast db**
- **show interface wideband-cable**
- **show cable multicast qos**

To verify the PCMM multicast gates, use the **show packetcable gate multimedia** command as shown in the following example:

```
Router# show packetcable gate multimedia multicast summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
134        Ca5/0/0      60.1.1.202     2.39.26.19     COMMIT    MM             4
Total number of Multimedia-MCAST gates = 1
Total Gates committed(since bootup or clear counter) = 1
```

To verify the PCMM IPv6 gates, use the **show packetcable gate multimedia ipv6**command as shown in the following example:

```
Router# show packetcable gate multimedia ipv6 summary
Load for five secs: 10%/1%; one minute: 9%; five minutes: 9%
Time source is NTP, 03:29:42.153 EST Mon Nov 9 2015

GateID     i/f                      SubscriberID                State   SFID(us) SFID(ds)
409        Ca5/0/2      2001:420:2C7F:FC38:58AF:E36A:80:213A   COMMIT             1326

16789      Ca5/0/2      2001:420:2C7F:FC38:AC40:A49A:F80A:8D0B COMMIT    1321
33177      Ca5/0/2      2001:420:2C7F:FC38:DD49:72A3:2ECC:8770 COMMIT             1322

49577      Ca5/0/2      2001:420:2C7F:FC38:485:31DF:C88B:E315  COMMIT    1308
65953      Ca5/0/2      2001:420:2C7F:FC38:5AB:AA0B:34AD:ACCF  COMMIT    1336
82337      Ca5/0/2      2001:420:2C7F:FC38:5AB:AA0B:34AD:ACCF  COMMIT             1337

98721      Ca5/0/2      2001:420:2C7F:FC38:5570:EF2E:7565:D36A COMMIT             1316

115097     Ca5/0/2      2001:420:2C7F:FC38:6009:EF26:F573:7356 COMMIT             1318

131489     Ca5/0/2      2001:420:2C7F:FC38:7D4A:BC50:3FD:CA7   COMMIT    1312
147873     Ca5/0/2      2001:420:2C7F:FC38:E83E:8259:AEF6:5624 COMMIT    1332
```

```
Total number of Multimedia gates = 10
Total Gates committed(since bootup or clear counter) = 1024
```

To verify all the PCMM client entries available with the multicast database, use the **show cable multicast db** command as shown in the following example:

```
Router# show cable multicast db client pcmm
Interface : Bundle1
Session (S,G) : (*,229.2.2.12)
Fwd Intf     Bundle Intf  Host Intf    CM MAC         CPE IP           Gate-ID SFID
Wi1/1/0:0    Bundle1      Ca5/0/0      0018.6852.8056 60.1.1.202       134 4
```

To verify multicast sessions on a specific wideband cable interface, use the **show interface wideband-cable** command as shown in the following example:

```
Router# show interface wideband-cable 1/1/0:0 multicast-sessions
Default Multicast Service Flow 3 on Wideband-Cable1/1/0:0
Multicast Group    : 229.2.2.12
         Source    : N/A
         Act GCRs  : 1
         Interface : Bu1                   State: A      GI: Bu1         RC: 0
  GCR       : GC   SAID    SFID    Key   GQC    GEn
                    512  8196    4       0     512    0
```

To verify the attribute-based assignment of service flows on a specific wideband cable interface, use the **show interface wideband-cable** command as shown in the following example:

```
Router# show interface wideband-cable 1/1/0:0
service-flow 4 verbose
Sfid                                  : 4
Mac Address                           : ffff.ffff.ffff
Type                                  : Secondary(Static)
Direction                             : Downstream
Current State                         : Active
Current QoS Indexes [Prov, Adm, Act]  : [4, 4, 4]
Active Time                           : 05:26
Required Attributes                   : 0x00000000
Forbidden Attributes                  : 0x00000000
Aggregate Attributes                  : 0x00000000
Multicast Sid                         : 8196
Traffic Priority                      : 0
Maximum Sustained rate                : 0 bits/sec
Maximum Burst                         : 3044 bytes
Minimum Reserved Rate                 : 250000 bits/sec
Minimum Packet Size                   : 0 bytes
Maximum Latency                       : 0 usecs
Peak Rate                             : 0 bits/sec
Admitted QoS Timeout                  : 200 seconds
Active QoS Timeout                    : 0 seconds
Packets                               : 0
Bytes                                 : 0
Rate Limit Delayed Packets            : 0
Rate Limit Dropped Packets            : 0
Current Throughput                    : 0 bits/sec, 0 packets/sec
Application Priority                  : 0
Low Latency App                       : No
Blaze/JIB3 DS Statistic Index         : 0
Forwarding Interface                  : Wi1/1/0:0
Classifiers: NONE
```

To verify that the PCMM-based MQoS gate controllers are created using the correct session ranges, use the **show cable multicast qos**command as shown in the following example:

```
Router# show cable multicast qos group-qos
Group QOS Index    Service Class    Control    Igmp Limit    Override  App
 DEFAULT           mcast_default     Aggregate  NO-LIMIT
 1                 SDV_SD            Single      ---          No        CLI
 512               SDV_HD            Single      ---          No        PCMM
```

High Availability Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia

Cisco IOS Release 12.2(33)SCA includes enhanced high availability support that enables the synchronization of PacketCable and PacketCable MultiMedia (PCMM) gates during switchover events on the Cisco CMTS router. This enhancement is enabled by default on the Cisco uBR10012 router and Cisco uBR7246VXR router.

This enhancement requires no additional configuration commands for line card redundancy in the Cisco N+1 Redundancy feature, nor the RPR+ Redundancy feature on the Cisco uBR10012 router. However, this functionality uses the existing per-interface HCCP commands that are used to associate the working and protect interfaces in the case of N+1 redundancy.

Debugging High Availability Stateful Switchover for PacketCable and PCMM

The **debug packetcable hccp** command enables debugging and troubleshooting functions on the Cisco CMTS router when PacketCable and PCMM features are supported in N+1 or RPR+ redundancy mode.

After the implementation of the PacketCable or PCMM feature, you will be able to connect to the standby line card and check if the gate information has been synchronized using the show packetcable gate summary command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debugpacketcablehccp** **Example:** `Router# debug packetcable hccp`	Enables debugging for gate synchronization within N+1 or RPR+ redundancy mode when they are operational on the network. To disable debugging, use the **no** form of this command.
Step 3	**showpacketcablegatesummary** **Example:** `Router# show packetcable gate summary`	Displays PacketCable HCCP information, supporting gate synchronization status and switchover information.

	Command or Action	Purpose
Step 4	**showhccpbrief** **Example:** `Router# show hccp brief`	Displays general information pertaining to N+1 redundancy on the Cisco CMTS router.

The following abbreviated example displays PacketCable gate synchronization information when debugging is enabled with the **debug packetcable hccp** command:

```
GateID    i/f     SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
Total number of  gates = 0
Total Gates committed(since bootup or clear counter) = 625
```

The following example displays additional information that tracks the activity as a call is made:

```
10:58:09: PktCbl(hccp): Grp 1 sync type=add from Cable5/0/0
10:58:09: PktCbl(hccp): Sync gate-add 38010 len=308
10:58:10: PktCbl(hccp): Grp 1 sync type=add from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-add 5242 len=308
10:58:10: Pktcbl(hccp): Gate=5242 written to service flow dir US SFID=1233
10:58:10: Pktcbl(hccp): Gate=5242 written to service flow dir DS SFID=1234
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 5242 len=24
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 5242 len=24
10:58:10: Pktcbl(hccp): Gate=38010 written to service flow dir US SFID=1235
10:58:32: PktCbl(hccp): Parse add gate 38010 sync_len=300 from 5/0 status 2
10:58:32: PktCbl(hccp): Parse add gate 5242 sync_len=300 from 5/0 status 2
10:58:32: PktCbl(hccp): Parse update gate 5242 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 5242 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:10: Pktcbl(hccp): Gate=38010 written to service flow dir DS SFID=1236
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:11: Pktcbl(hccp): Gate=38010 written to service flow dir US SFID=1235
10:58:11: Pktcbl(hccp): Gate=38010 written to service flow dir DS SFID=1236
10:58:11: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:11: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:11: Pktcbl(hccp): Gate=5242 written to service flow dir US SFID=1233
10:58:11: Pktcbl(hccp): Gate=5242 written to service flow dir DS SFID=1234
10:58:11: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:11: PktCbl(hccp): Sync gate-update 5242 len=24
10:58:34: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:34: PktCbl(hccp): Parse update gate 5242 sync_len=16
****** CALL IS ACTIVE **** SHOW GATE ON PRE *************
sch_3# gate
GateID    i/f     SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
5242      Ca5/0/0 7.7.1.254      1.10.90.1      COMMIT    DQoS  1233     1234
38010     Ca5/0/0 7.7.1.252      1.10.90.1      COMMIT    DQoS  1235     1236
Total number of  gates = 2
Total Gates committed(since bootup or clear counter) = 627
```

The following is a sample output of the **show hccp** command:

```
Router# show hccp brief
```

```
Interface Config    Grp Mbr Status          WaitToResync    WaitToRestore
Ca5/0/0   Working   1   1   active          never
Ca8/0/0   Protect   1   1   standby
Ca8/0/0   Protect   1   2   non-functional
Ca8/1/0   Protect   3   1   non-functional
Ca8/1/1   Protect   4   1   non-functional
sch_3#
```

PacketCable and PCMM with Admission Control

A PacketCable or PacketCable Multimedia network contains a number of components that benefit from Admission Control QoS. Admission Control manages and optimizes QoS for PacketCable and PCMM in these ways:

- QoS (based on DOCSIS 1.1 or later versions) for voice and data
- Cable modem registration
- CMS
- Gateway controllers (GC)
- Record keeping servers (RKS)
- Video telephony

When configuring Admission Control with either PacketCable or PCMM, PacketCable or PCMM must be fully operational on the Cisco CMTS headend prior to gaining the benefits from Admission Control.

For Admission Control configuration information, refer to the following documents:

- Admission Control for the Cisco Cable Modem Termination System
- Service Flow Admission Control for the Cisco Cable Modem Termination System

Voice MGPI Support

The multiple grants per interval (MGPI) feature, introduced in Cisco IOS Release 12.2(33)SCF, enables the Cisco CMTS router to map multiple PacketCable or PacketCable Multimedia gates (application flows) to a single DOCSIS service flow using UGS traffic profiles of the same cable modem. In other words, the Cisco CMTS router increases the number of grants per interval for each application flow based on a single service flow, resulting in multiple grants per interval.

The MGPI feature supports the flow-aggregated voice MGPI functionality based on CableLabs PacketCable Specification (PKT-SP-MM-I05-091029). The flow-aggregated MGPI functionality allows the application manager to use the UGS traffic profile to explicitly set the number of grants per interval and place several application flows on a single gate. This results in an aggregated view for event messages, volume, and time usage limits.

Voice Support Over DOCSIS 3.0 E-MTAs

Beginning with Cisco IOS Release 12.2(33)SCF, PacketCable and PCMM services are supported on embedded multimedia terminal adapters (E-MTAs). An E-MTA is a network element that contains the interface to a physical voice device, a network interface, and all signaling and encapsulation functions required for the VoIP transport, class features signaling, and QoS signaling.

PacketCable and PCMM Call Trace

The PacketCable and PCMM call trace functionality is introduced in Cisco IOS Release 12.2(33)SCF for advanced debugging of PacketCable and PCMM calls. To effectively capture signaling information, this functionality buffers signaling for a configured number of PacketCable or PCMM gates. By default, only ten user-configured gate traces are saved in a buffer. After the specified number is reached, any subsequent gate signaling information does not get buffered. When one of the gates being traced is deleted, gate signaling of a new gate is buffered.

Use the **cable dynamic-qos trace** command in global configuration mode to enable the call trace functionality for PacketCable and PacketCable Multimedia gates on the Cisco CMTS router. You will have to specify the number of subscribers for whom call trace needs to be enabled.

Verifying Call Traces

Use the following commands to verify PacketCable and PCMM call trace functionality on the Cisco CMTS router:

- **debug cable dynamic-qos subscriber**
- **debug cable dynamic-qos trace**
- **show cable dynamic-qos trace**

To verify debugging information for all the configured subscribers on the Cisco CMTS router, use the **debug cable dynamic-qos subscriber** command as shown in the following example:

```
Router# debug cable dynamic-qos subscriber
CMTS dynqos subscriber debugging is on ubr10k#
*Mar 17 08:32:27.135: Pktcbl(gdb): Created gate IE on Cable7/1/0, gateid = 10804
2
*Mar 17 08:32:27.135: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.135: Pktcbl(mm): Change profile 0 qos 0
*Mar 17 08:32:27.135: Pktcbl(gdb): IPC timer [id 108042] [10000 msec]
*Mar 17 08:32:27.135: Pktcbl(gdb): Started gate [id 108042] timer [type 8] [1000
0 msec]
*Mar 17 08:32:27.135: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.135: Pktcbl(gdb): MM gate spec: t1:200, t2:0, t3:0, t4:0
*Mar 17 08:32:27.135: Pktcbl(gdb): MM traffic profile type: 6
*Mar 17 08:32:27.135: Pktcbl(gdb): MM Authorized Profile
*Mar 17 08:32:27.135: Pktcbl(gdb): MM Reserved Profile
*Mar 17 08:32:27.135: Pktcbl(gdb): MM Committed Profile
*Mar 17 08:32:27.135: Classifier prototype: 1, src: 9.9.1.95, dest: 2.39.26.11,
src port: 0, dest port: 0
*Mar 17 08:32:27.179: Pktcbl(mm): Received gate-set IPC RSP from LC for gate 108
042 rsp 1 state new(4) old(2)
*Mar 17 08:32:27.179: Pktcbl(gdb): Cancelled gate [id 108042] timer [type 8]
*Mar 17 08:32:27.179: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.179: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.179: Pktcbl(gdb): Started gate [id 108042] timer [type 3] [0 ms
ec]
```

```
*Mar 17 08:32:27.179: PktCbl(d2r): extract id: gate=108042, resource=74
*Mar 17 08:32:27.179: PktCbl(d2r): extract id: gate=108042, resource=74
*Mar 17 08:32:27.179: Pktcbl(gdb): TOS Overwrite gate spec info,gate_id=108042 d
ir=1 gie=26DD5C98
*Mar 17 08:32:27.179: Pktcbl(gdb): TOS Overwrite Gate=108042 DSCP=0xD0 mask=0xF
*Mar 17 08:32:27.179: PktCbl(d2r): extract id: gate=108042, resource=74
*Mar 17 08:32:27.179: PktCbl(mm-r2d): DSA-ACK notification received on RP, gatei
d 108042 sfid 74
*Mar 17 08:32:27.179: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.183: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:27.183: Pktcbl(mm): Building GCP message, added obj TRANSACTION
ubr10k# ID      ; len:8 padding:0
*Mar 17 08:32:27.183: Pktcbl(mm): Building GCP message, added obj AM ID
      ; len:8 padding:0
*Mar 17 08:32:27.183: Pktcbl(mm): Building GCP message, added obj SUBSCRIBER ID
      ; len:8 padding:0
*Mar 17 08:32:27.183: Pktcbl(mm): Building GCP message, added obj GATE ID
      ; len:8 padding:0
*Mar 17 08:32:27.183: Pktcbl(mm): Building GCP message, added obj OPAQUE
      ; len:12 padding:0
*Mar 17 08:32:27.183: Pktcbl(mm): Built GCP message, GATE SET ACK        , lengt
h: 44, copsLen 72
*Mar 17 08:32:27.183:  --- Pktcbl: Sending GCP message ------
*Mar 17 08:32:27.183: TRANSACTION ID       : Object.[snum/stype/len 1/1/8]
*Mar 17 08:32:27.183:     transaction id   : 0x1
*Mar 17 08:32:27.183:     gcp cmd          : 5 (GATE SET ACK)
*Mar 17 08:32:27.183: AM ID                : Object.[snum/stype/len 2/1/8]
*Mar 17 08:32:27.183:     AM ID            : 0x1 (0/1)
*Ma
ubr10k#r 17 08:32:27.183: SUBSCRIBER ID        : Object.[snum/stype/len 3/1/8]
*Mar 17 08:32:27.183:     Addr             : 21.21.2.10
*Mar 17 08:32:27.183: GATE ID              : Object.[snum/stype/len 4/1/8]
*Mar 17 08:32:27.183:     GateID           : 108042 (0x1A60A)
*Mar 17 08:32:27.183: OPAQUE               : Object.[snum/stype/len 11/1/12]
*Mar 17 08:32:27.183:     data             : [31 32 33 34 00 00 00 00 ]
*Mar 17 08:32:27.183:  ---------------------------------------
SLOT 7/1: Mar 17 08:32:27.152: Pktcbl(gdb): Gate ID 108042 not found in gdb, pkt
cbl_find_gate_ie.
SLOT 5/0: Mar 17 08:32:27.151: Pktcbl(gdb): Gate ID 108042 not found in gdb, pkt
cbl_find_gate_ie.
ubr10k#
*Mar 17 08:32:56.656: Pktcbl(mm): Received GATE SET message, tid=0x2
*Mar 17 08:32:56.656: --- Pktcbl(mm): Received GCP message ------
*Mar 17 08:32:56.656: TRANSACTION ID       : Object.[snum/stype/len 1/1/8]
*Mar 17 08:32:56.656:     transaction id   : 0x2
*Mar 17 08:32:56.656:     gcp cmd          : 4 (GATE SET)
*Mar 17 08:32:56.656: AM ID                : Object.[snum/stype/len 2/1/8]
*Mar 17 08:32:56.656:     AM ID            : 0x1 (0/1)
*Mar 17 08:32:56.656: SUBSCRIBER ID        : Object.[snum/stype/len 3/1/8]
*Mar 17 08:32:56.656:     Addr             : 21.21.2.10
*Mar 17 08:32:56.656: GATE ID              : Object.[snum/stype/len 4/1/8]
*Mar 17 08:32:56.656:     GateID           : 108042 (0x1A60A)
*Mar 17 08:32:56.656: GATE SPEC            : Object.[snum/stype/len 5/1/16]
*Mar 17 08:32:56.656:     flag             : 0x3
*Mar 17 08:32:56.656:     dscp             : 0xD8
*Mar 17 08:32:56.656:     dscp tos mask    : 0xF0
*Mar 17 08:32:56.656:     Timers  t1       : 0,  t2 : 0
*Mar 17 08:32:56.656:             t3       : 0,  t4 : 0
*Mar 17 08:32:56.656:     session class    : 0x0
*Mar 17 08:32:56.656: TRAFFIC PROFILE      : Object.[snum/stype/len 7/6/56]
*Mar 17 08:32:56.656:     envelope         : 0x7
*Mar 17 08:32:56.656:     service number   : 0x0
*Mar 17 08:32:56.656:     Authorized :
*Mar 17 08:32:56.656: Request Xmit Policy: 0x17F
*Mar 17 08:32:56.656: Grant size         : 232
*Mar 17 08:32:56.656: Grant Per Interval : 2
*Mar 17 08:32:56.656: Grant Interval     : 20000
*Mar 17 08:32:56.656: Tolerated Jitter   : 800
*Mar 17 08:32:56.656: Required Mask      : 0
*Mar 17 08:32:56.656: Forbidden Mask     : 0
*Mar 17 08:32:56.656: Aggr Rule Mask     : 0
*Mar 17 08:32:56.656:     Reserved   :
*Mar 17 08:32:56.656: Request Xmit Policy: 0x17F
```

```
*Mar 17 08:32:56.656: Grant size         : 232
*Mar 17 08:32:56.656: Grant Per Interval : 2
*Mar 17 08:32:56.656: Grant Interval     : 20000
*Mar 17 08:32:56.656: Tolerated Jitter   : 800
*Mar 17 08:32:56.656: Required Mask      : 0
*
ubr10k#Mar 17 08:32:56.656: Forbidden Mask     : 0
*Mar 17 08:32:56.656: Aggr Rule Mask     : 0
*Mar 17 08:32:56.656: CLASSIFIER           : Object.[snum/stype/len 6/1/24]
*Mar 17 08:32:56.656:     protocol         : 1
*Mar 17 08:32:56.656:     dscp             : 0x0
*Mar 17 08:32:56.656:     dscp tos mask    : 0x0
*Mar 17 08:32:56.656:     src/port         : 9.9.1.95 0
*Mar 17 08:32:56.656:     dest/port        : 2.39.26.11 0
*Mar 17 08:32:56.656:     priority         : 64
*Mar 17 08:32:56.656: CLASSIFIER           : Object.[snum/stype/len 6/1/24]
*Mar 17 08:32:56.656:     protocol         : 1
*Mar 17 08:32:56.656:     dscp             : 0x0
*Mar 17 08:32:56.656:     dscp tos mask    : 0x0
*Mar 17 08:32:56.656:     src/port         : 9.9.1.43 0
*Mar 17 08:32:56.656:     dest/port        : 2.39.26.19 0
*Mar 17 08:32:56.656:     priority         : 64
*Mar 17 08:32:56.656: OPAQUE               : Object.[snum/stype/
ubr10k#len 11/1/12]
*Mar 17 08:32:56.656:     data             : [31 32 33 34 00 00 00 00 ]
*Mar 17 08:32:56.656: ---------------------------------------
*Mar 17 08:32:56.656:  Backup gate IE [108042]
*Mar 17 08:32:56.656: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:56.656: Pktcbl(mm): Change profile 1 qos 1
*Mar 17 08:32:56.656: Pktcbl(gdb): IPC timer [id 108042] [10000 msec]
*Mar 17 08:32:56.656: Pktcbl(gdb): Started gate [id 108042] timer [type 8] [1000
0 msec]
*Mar 17 08:32:56.656: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:56.656: Pktcbl(gdb): MM gate spec: t1:200, t2:0, t3:0, t4:0
*Mar 17 08:32:56.656: Pktcbl(gdb): MM traffic profile type: 6
*Mar 17 08:32:56.656: Pktcbl(gdb): MM Authorized Profile
*Mar 17 08:32:56.660: Pktcbl(gdb): MM Reserved Profile
*Mar 17 08:32:56.660: Pktcbl(gdb): MM Committed Profile
*Mar 17 08:32:56.660: Classifier prototype: 1, src: 9.9.1.95, dest: 2.39.26.11,
src port: 0, dest port: 0
*Mar 17 08:32:56.660: Classifier prototype: 1, src: 9.9.1.43, dest: 2.39.26.19,
src port: 0, dest port: 0
*Mar 17 08:32:56.696: Pktcbl(mm): Received gate-set IPC RSP from LC for gate 108
042 rsp 1 state new(4) old(4)
*Mar 17 08:32:56.696: Pktcbl(gdb): Cancelled gate [id 108042] timer [type 8]
*Mar 17 08:32:56.696: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:56.696: Pktcbl(gdb): Started gate [id 108042] timer [type 3] [0 ms
ec]
*Mar 17 08:32:56.696: Pktcbl(gdb): Cleanup saved gate IE info, gate(108042)
*Mar 17 08:32:56.696: PktCbl(d2r): extract id: gate=108042, resource=74
*Mar 17 08:32:56.696: Pktcbl(gdb): TOS Overwrite gate spec info,gate_id=108042 d
ir=1 gie=26DD5C98
*Mar 17 08:32:56.696: Pktcbl(gdb): TOS Overwrite Gate=108042 DSCP=0xD0 mask=0xF
*Mar 17 08:32:56.696: PktCbl(d2r): extract id: gate=108042, resource=74
*Mar 17 08:32:56.696: PktCbl(mm-r2d): DSA-ACK notification received on RP, gatei
d 108042 sfid 74
*Mar 17 08:32:56.696: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:56.696: Pktcbl(gdb): Found Cable7/1/0 for Gate=108042 21.21.2.10
*Mar 17 08:32:56.696: Pktcbl(mm): Building GCP message, added obj TRANSACTION ID
      ; len:8 padding:0
*Mar 17 08:32:56.696: Pktcbl(mm): Building GCP message, added obj AM ID
      ; len:8 padding:0
*Mar 17 08:32:56.696: Pktcbl(mm): Building GCP message, added obj SUBSCRIBER ID
      ; len:8 padding:0
*Mar 17 08:32:56.696: Pktcbl(mm): Building GCP message, added obj GATE ID
      ; len:8 padding:0
*Mar 17 08:32:56.696: Pktcbl(mm): Building GCP message, added obj OPAQUE
      ; len:12 padding:0
*Mar 17 08:32:56.696: Pktcbl(mm): Built GCP message, GATE SET ACK        , lengt
h: 44, copsLen 72
*Mar 17 08:32:56.696:  --- Pktcbl: Sending GCP message ------
*Mar 17 08:32:56.696: TRANSACTION ID       : Object.[snum/stype/len 1/1/8]
*Mar 17 08:32:56.696:     transaction id   : 0x2
```

```
*Mar 17 08:32:56.696:     gcp cmd          : 5 (GATE SET ACK)
*Mar 17 08:32:56.696: AM ID                : Object.[snum/stype/len 2/1/8]
*Mar 17 08:32:56.696:     AM ID            : 0x1 (0/1)
*Mar 17 08:32:56.696: SUBSCRIBER ID        : Object.[snum/stype/len 3/1/8]
*Mar 17 08:32:56.696:     Addr             : 21.21.2.10
*Mar 17 08:32:56.696: GATE ID              : Object.[snum/stype/len 4/1/8]
*Mar 17 08:32:56.696:     GateID           : 108042 (0x1A60A)
*Mar 17 08:32:56.696: OPAQUE               : Object.[snum/stype/len 11/1/12]
*Mar 17 08:32:56.696:     data             : [31 32 33 34 00 00 00 00 ]
*Mar 17 08:32:56.696:  ---------------------------------------
```

To verify call trace debugging information for all the configured subscribers on the Cisco CMTS router, use the **debug cable dynamic-qos trace** command as shown in the following example:

```
Router# debug cable dynamic-qos trace
CMTS dynqos trace debugging is on ubr10k#
*Mar 17 02:43:05.448: Pktcbl(mm): Received GATE SET message, tid=0x2
*Mar 17 02:43:05.448: --- Pktcbl(mm): Received GCP message ------
*Mar 17 02:43:05.448: TRANSACTION ID       : Object.[snum/stype/len 1/1/8]
*Mar 17 02:43:05.448:     transaction id   : 0x2
*Mar 17 02:43:05.448:     gcp cmd          : 4 (GATE SET)
*Mar 17 02:43:05.448: AM ID                : Object.[snum/stype/len 2/1/8]
*Mar 17 02:43:05.448:     AM ID            : 0x1 (0/1)
*Mar 17 02:43:05.448: SUBSCRIBER ID        : Object.[snum/stype/len 3/1/8]
*Mar 17 02:43:05.448:     Addr             : 21.21.2.10
*Mar 17 02:43:05.448: GATE ID              : Object.[snum/stype/len 4/1/8]
*Mar 17 02:43:05.452:     GateID           : 58886 (0xE606)
*Mar 17 02:43:05.452: GATE SPEC            : Object.[snum/stype/len 5/1/16]
*Mar 17 02:43:05.452:     flag             : 0x3
*Mar 17 02:43:05.452:     dscp             : 0xD8
*Mar 17 02:43:05.452:     dscp tos mask    : 0xF0
*Mar 17 02:43:05.452:     Timers  t1       : 0,  t2 : 0
*Mar 17 02:43:05.452:             t3       : 0,  t4 : 0
*Mar 17 02:43:05.452:     session class    : 0x0
*Mar 17 02:43:05.452: TRAFFIC PROFILE      : Object.[snum/stype/len 7/6/56]
*Mar 17 02:43:05.452:     envelope         : 0x7
*Mar 17 02:43:05.452:     service number   : 0x0
*Mar 17 02:43:05.452:     Authorized :
*Mar 17 02:43:05.452: Request Xmit Policy: 0x17F
*Mar 17 02:43:05.452: Grant size         : 232
*Mar 17 02:43:05.452: Grant Per Interval : 2
*Mar 17 02:43:05.452: Grant Interval     : 20000
*Mar 17 02:43:05.452: Tolerated Jitter   : 800
*Mar 17 02:43:05.452: Required Mask      : 0
*Mar 17 02:43:05.452: Forbidden Mask     : 0
*Mar 17 02:43:05.452: Aggr Rule Mask     : 0
*Mar 17 02:43:05.452:     Reserved   :
*Mar 17 02:43:05.452: Request Xmit Policy: 0x17F
*Mar 17 02:43:05.452: Grant size         : 232
*Mar 17 02:43:05.452: Grant Per Interval : 2
*Mar 17 02:43:05.452: Grant Interval     : 20000
*Mar 17 02:43:05.452: Tolerated Jitter   : 800
*Mar 17 02:43:05.452: Required Mask      : 0
*Ma
ubr10k#r 17 02:43:05.452: Forbidden Mask     : 0
*Mar 17 02:43:05.452: Aggr Rule Mask     : 0
*Mar 17 02:43:05.452: CLASSIFIER           : Object.[snum/stype/len 6/1/24]
*Mar 17 02:43:05.452:     protocol         : 1
*Mar 17 02:43:05.452:     dscp             : 0x0
*Mar 17 02:43:05.452:     dscp tos mask    : 0x0
*Mar 17 02:43:05.452:     src/port         : 9.9.1.95 0
*Mar 17 02:43:05.452:     dest/port        : 2.39.26.11 0
*Mar 17 02:43:05.452:     priority         : 64
*Mar 17 02:43:05.452: CLASSIFIER           : Object.[snum/stype/len 6/1/24]
*Mar 17 02:43:05.452:     protocol         : 1
*Mar 17 02:43:05.452:     dscp             : 0x0
*Mar 17 02:43:05.452:     dscp tos mask    : 0x0
*Mar 17 02:43:05.452:     src/port         : 9.9.1.43 0
*Mar 17 02:43:05.452:     dest/port        : 2.39.26.19 0
*Mar 17 02:43:05.452:     priority         : 64
*Mar 17 02:43:05.452: OPAQUE               : Object.[snum/stype/le
ubr10k#n 11/1/12]
```

```
*Mar 17 02:43:05.452:     data             : [31 32 33 34 00 00 00 00 ]
*Mar 17 02:43:05.452: ------------------------------------
*Mar 17 02:43:05.452:  Backup gate IE [58886]
*Mar 17 02:43:05.452: Pktcbl(gdb): Found Cable7/1/0 for Gate=58886 21.21.2.10
*Mar 17 02:43:05.452: Pktcbl(mm): Change profile 1 qos 1
*Mar 17 02:43:05.452: Pktcbl(gdb): IPC timer [id 58886] [10000 msec]
*Mar 17 02:43:05.452: Pktcbl(gdb): Started gate [id 58886] timer [type 8] [10000
 msec]
*Mar 17 02:43:05.452: Pktcbl(gdb): Found Cable7/1/0 for Gate=58886 21.21.2.10
*Mar 17 02:43:05.452: Pktcbl(gdb): MM gate spec: t1:200, t2:0, t3:0, t4:0
*Mar 17 02:43:05.452: Pktcbl(gdb): MM traffic profile type: 6
*Mar 17 02:43:05.452: Pktcbl(gdb): MM Authorized Profile
*Mar 17 02:43:05.452: Pktcbl(gdb): MM Reserved Profile
*Mar 17 02:43:05.452: Pktcbl(gdb): MM Committed Profile
*Mar 17 02:43:05.452: Classifier prototype: 1, src: 9.9.1.95, dest: 2.39.26.11,
src port: 0, dest port: 0
*Mar 17 02:43:05.452: Classifier prototype: 1, src: 9.9.1.43, dest: 2.39.26.19,
src port: 0, dest port: 0
*Mar 17 02:43:05.480: Pktcbl(mm): Received gate-set IPC RSP from LC for gate 588
86 rsp 1 state new(4) old(4)
*Mar 17 02:43:05.480: Pktcbl(gdb): Cancelled gate [id 58886] timer [type 8]
*Mar 17 02:43:05.480: Pktcbl(gdb): Found Cable7/1/0 for Gate=58886 21.21.2.10
*Mar 17 02:43:05.480: Pktcbl(gdb): Started gate [id 58886] timer [type 3] [0 mse
c]
*Mar 17 02:43:05.480: Pktcbl(gdb): Cleanup saved gate IE info, gate(58886)
*Mar 17 02:43:05.484: PktCbl(d2r): extract id: gate=58886, resource=64
*Mar 17 02:43:05.484: Pktcbl(gdb): TOS Overwrite gate spec info,gate_id=58886 di
r=1 gie=265BDB84
*Mar 17 02:43:05.484: Pktcbl(gdb): TOS Overwrite Gate=58886 DSCP=0xD0 mask=0xF
*Mar 17 02:43:05.484: PktCbl(d2r): extract id: gate=58886, resource=64
*Mar 17 02:43:05.484: PktCbl(mm-r2d): DSA-ACK notification received on RP, gatei
d 58886 sfid 64
*Mar 17 02:43:05.484: Pktcbl(gdb): Found Cable7/1/0 for Gate=58886 21.21.2.10
*Mar 17 02:43:05.484: Pktcbl(gdb): Found Cable7/1/0 for Gate=58886 21.21.2.10
*Mar 17 02:43:05.484: Pktcbl(mm): Building GCP message, added obj TRANSACTION ID
      ; len:8 padding:0
*Mar 17 02:43:05.484: Pktcbl(mm): Building GCP message, added obj AM ID
      ; len:8 padding:0
*Mar 17 02:43:05.484: Pktcbl(mm): Building GCP message, added obj SUBSCRIBER ID
      ; len:8 padding:0
*Mar 17 02:43:05.484: Pktcbl(mm): Building GCP message, added obj GATE ID
      ; len:8 padding:0
*Mar 17 02:43:05.484: Pktcbl(mm): Building GCP message, added obj OPAQUE
      ; len:12 padding:0
*Mar 17 02:43:05.484: Pktcbl(mm): Built GCP message, GATE SET ACK        , lengt
h: 44, copsLen 72
*Mar 17 02:43:05.484:  --- Pktcbl: Sending GCP message ------
*Mar 17 02:43:05.484: TRANSACTION ID       : Object.[snum/stype/len 1/1/8]
*Mar 17 02:43:05.484:     transaction id   : 0x2
*Mar 17 02:43:05.484:     gcp cmd          : 5 (GATE SET ACK)
*Mar 17 02:43:05.484: AM ID                : Object.[snum/stype/len 2/1/8]
*Mar 17 02:43:05.484:     AM ID            : 0x1 (0/1)
*Mar 17 02:43:05.484: SUBSCRIBER ID        : Object.[snum/stype/len 3/1/8]
*Mar 17 02:43:05.484:     Addr             : 21.21.2.10
*Mar 17 02:43:05.484: GATE ID              : Object.[snum/stype/len 4/1/8]
*Mar 17 02:43:05.484:     GateID           : 58886 (0xE606)
*Mar 17 02:43:05.484: OPAQUE               : Object.[snum/stype/len 11/1/12]
*Mar 17 02:43:05.484:     data             : [31 32 33 34 00 00 00 00 ]
*Mar 17 02:43:05.484:  ------------------------------------
```

To verify the number of subscribers for whom call trace is enabled on the Cisco CMTS router, use the **show cable dynamic-qos trace** command as shown in the following example:

```
Router# show cable dynamic-qos trace
Total number of subscribers: 0
Max configured number of subscribers: 12
```

Verifying PacketCable and PCMM Statistics

Use the following commands to verify PacketCable and PCMM statistics on the Cisco CMTS router:

- **show interface cable dynamic-service statistics**
- **show interface cable packetcable statistics**
- **show packetcable cms**

To verify dynamic service statistics based on the cable interface, use the show interface cable dynamic-service statistics command as shown in the following example:

```
Router# show interface cable 7/1/0 dynamic-service statistics
  Upstream        Downstream
DSA REQ      0               5
DSA RSP      5               0
DSA ACK      0               5
DSC REQ      0               5
DSC RSP      5               0
DSC ACK      0               5
DSD REQ      0               0
DSD RSP      0               0
Retransmission counts
             Upstream        Downstream
DSA REQ      0               0
DSA RSP      0               0
DSA ACK      0               0
DSC REQ      0               5
DSC RSP      5               0
DSC ACK      0               0
DSD REQ      0               0
DSD RSP      0               0
```

To verify PacketCable IPC statistics based on the cable interface, use the show interface cable packetcable statistics command as shown in the following example:

```
Router# show interface cable 7/1/0 packetcable statistics
Packetcable IPC Statistics on RP
Msg   create     gate       gate       gate set   dsd
      gie        set        del        notify     notify
Sent  0          10         0          0          0
Rcvd  0          0          0          10         0
Packetcable IPC Statistics on LC
Msg   create     gate       gate       gate set   dsd
      gie        set        del        notify     notify
Sent  0          0          0          10         0
Rcvd  0          10         0          0          0
```

To verify all gate controllers that are currently connected to the PacketCable client, use the show packetcable cms command as shown in the following example:

```
Router# show packetcable cms
GC-Addr        GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2     47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19     55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
```

To verify all gate controllers including the COPS servers for which the PacketCable connection is gone down, use the **show packetcable cms** command with the all keyword as shown in the following example:

```
Router# show packetcable cms all
GC-Addr        GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2     47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19     55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
1.10.30.22     42307    2.39.34.1      0x0       /0    4.0   0    0   0
```

To verify gate controller statistics, use the **show packetcable cms** command with the keyword, verbose, as shown in the following example:

```
Router# show packetcable cms verbose
Gate Controller
     Addr         :     1.100.30.2
```

```
      Port          :     47236
      Client Addr   :     2.39.34.1
      COPS Handle   :     0x2FF9E268
      Version       :     4.0
      Statistics    :
         gate del =  0  gate del ack =  0   gate del err = 0
         gate info = 0  gate info ack = 0  gate info err = 0
         gate open =  0  gate report state = 0
         gate set =  0  gate set ack =  0   gate set err = 0
         gate alloc = 0 gate alloc ack = 0  gate alloc err = 0
         gate close =  0
Gate Controller
      Addr          :     2.39.26.19
      Port          :     55390
      Client Addr   :     2.39.34.1
      COPS Handle   :     0x2FF9D890
      Version       :     1.0
      Statistics    :
         gate del =  0  gate del ack =  0   gate del err = 0
         gate info = 0  gate info ack = 0  gate info err = 0
         gate open =  0  gate report state = 0
         gate set =  2  gate set ack =  2   gate set err = 0
         PCMM Timers Expired
         Timer T1 =  0  Timer T2 =  0 Timer T3 = 0 Timer T4 = 0
GC-Addr         GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2      47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19      55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CMTS commands	*Cisco CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
N+1 redundancy	*N+1 Redundancy for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun_ps2209_TSD_Products_Configuration_Guide_Chapter.html
NTP or SNTP Configuration	To configure the Cisco CMTS router to use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to set its system clock, see the "Performing Basic System Management" chapter in the "System Management" section of the Cisco IOS Configuration Fundamentals Configuration Guide.

Standards

Standards[88]	Title
PKT-SP-MM-I06-110629	PacketCable™ Specification Multimedia Specification
ITU X.509 V3	*International Telecommunications Union (ITU) X.509 Version 3.0* standard
PKT-EM-I03-011221	*PacketCable™ Event Message Specification*
PKT-SP-DQOS-I04-021018	*PacketCable™ Dynamic Quality-of-Service Specification*
PKT-SP-EC-MGCP-I04-011221	*PacketCable™ Network-Based Call Signaling Protocol Specification*
PKT-SP-ESP-I01-991229	*PacketCable™ Electronic Surveillance Specification*
PKT-SP-ISTP-I02-011221	*PacketCable™ Internet Signaling Transport Protocol (ISTP) Specification*
PKT-SP-PROV-I03-011221	*PacketCable™ MTA Device Provisioning Specification*

88 Not all supported standards are listed.

MIBs

MIBs	MIBs Link
No new or changed MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 1510	*The Kerberos Network Authentication Service (V5)*
RFC 2138	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2205	*Resource ReSerVation Protocol (RSVP)*

RFCs	Title
RFC 2327	*SDP: Session Description Protocol*
RFC 2748	*The COPS (Common Open Policy Service) Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PacketCable and PacketCable Multimedia on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 132: Feature Information for PacketCable and PacketCable Multimedia on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
PacketCable	12.2(8)BC2	This feature was introduced on the Cisco uBR7246VXR router on the Cisco uBR-MC28U cable interface line card. The following commands were introduced: • **clear packetcable gate counter commit** • **debug packetcable gate** • **packetcable** • **packetcable gate maxcount** • **packetcable timer** • **show packetcable gate** • **show packetcable gate counter commit** • **show packetcable global**
PacketCable	12.2(11)BC1	Support was added for version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116) and for configuring the Event Message Element ID for the Cisco uBR7246VXR router. The **packetcable element-id** command was introduced.
PacketCable	12.2(11)BC2	Support was added for the **packetcable authorize vanilla-docsis-mta** command, which allows both PacketCable and non-PacketCable DOCSIS UGS service flows when PacketCable is enabled. The **show packetcable global** command was also enhanced to show whether non-PacketCable UGS service flows are enabled, and the T2 and T5 timers were removed from the display to conform to the requirements of the PacketCable Engineering Change Notice (ECN) 02148.

Feature Name	Releases	Feature Information
PacketCable	12.2(15)BC1	PacketCable 1.x supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router. In addition, several **debug packetcable** commands have been added or enhanced. The following commands were introduced: • **debug packetcable ipc** • **debug packetcable subscriber**
PacketCable	12.2(15)BC2	The following commands were introduced: • **debug packetcable hccp** • **show packetcable event**
PacketCable	12.3(9a)BC	This feature was integrated into Cisco IOS Release 12.3(9a)BC. Support was added for Packet Cable 1.0 with CALEA on the Cisco uBR10012 router.

Feature Name	Releases	Feature Information
PacketCable Multimedia	12.3(13a)BC	This feature was introduced for the Cisco uBR7246VXR router and Cisco uBR10012 router. The following PacketCable 1.x features introduced for the Cisco uBR7246VXR router and Cisco uBR10012 router: • PacketCable Emergency 911 Cable Interface Line Card Prioritization • PacketCable Emergency 911 Services Listing and History The following commands were introduced or modified: • **debug packetcable gate docsis-mapping** • **debug packetcable gate event** • **packetcable multimedia** • **packetcable timer multimedia t1** • **show packetcable gate**
PacketCable and PacketCable Multimedia	12.3(21)BC	The following features were introduced on the Cisco CMTS routers: • High Availability Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia • PacketCable Client Accept Timeout
PacketCable and PacketCable Multimedia	12.2(33)SCA	These features were integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.

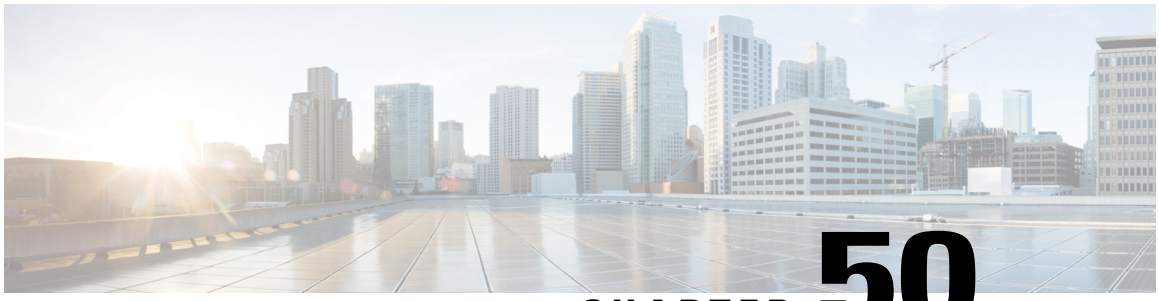
Feature Name	Releases	Feature Information
PacketCable	12.2(33)SCB	The following features were introduced on the Cisco CMTS routers: • PacketCable Subscriber ID • Dynamic Service Transaction ID is introduced to conform to the requirements of the new transaction ID allocation algorithm for dynamic services on CMTS (DOCSIS ECN - RFIv2.0-N-04.0147-1.) **Note** The PacketCable Subscriber ID feature is not supported in Cisco IOS Release 12.2(33)SCA. However, it is supported beginning in Cisco IOS Release 12.2(33)SCB. The following commands were introduced or modified: • **packetcable gate send-subscriberID** • **show cable calls**
PacketCable	12.2(33)SCD	The PacketCable functionality was extended to Cisco uBR7200 series routers. The **clear packetcable rks** command was introduced.

Feature Name	Releases	Feature Information
Multicast Session Range	12.2(33)SCE	Support for the multicast session range configuration was added in Cisco IOS Release 12.2(33)SCE. The following sections provide information about this feature: • Configuring a PCMM Multicast Session Range, on page 1324 • Verifying PCMM Operations, on page 1326 The following commands were introduced or modified: • **cable multicast source pcmm** • **show packetcable gate multimedia** • **show cable multicast db** • **show cable multicast qos**
PacketCable Subscriber ID	12.2(33)SCE	The PacketCable Subscriber ID feature includes support for IPv6 addresses in Cisco IOS Release 12.2(33)SCE. The following commands were introduced or modified: • **show packetcable gate ipv6** • **show packetcable gate** • **show packetcable event**

Feature Name	Releases	Feature Information
Call Trace	12.2(33)SCF	The PacketCable and PCMM call trace functionality was introduced for advanced debugging of PacketCable and PCMM calls. The following section provides information about this feature: • Voice MGPI Support, on page 1330 The following commands were introduced or modified: • **cable dynamic-qos trace** • **debug cable dynamic-qos subscriber** • **debug cable dynamic-qos trace** • **show cable dynamic-qos trace**
Voice MGPI Support and Statistics	12.2(33)SCF	The MGPI feature enables the Cisco CMTS router to map multiple PacketCable or PCMM gates to a single DOCSIS service flow using UGS traffic profiles of the same cable modem. The following commands were introduced or modified: • **show interface cable dynamic-service statistics** • **show interface cable packetcable statistics** • **show packetcable cms**
PCMM IPv6 Voice	12.2(33)SCJ	This feature was introduced on the Cisco CMTS routers.
PCMM Multicast	12.2(33)SCJ	This feature was introduced on the Cisco CMTS routers.

PART VIII

Quality of Service Features



CHAPTER 50

Default DOCSIS 1.0 ToS Overwrite

First Published: February 14, 2008

Last Updated: May 10, 2010

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Default DOCSIS 1.0 ToS Overwrite feature for the Cisco Cable Modem Termination System (CMTS). This feature eliminates the need to create multiple QoS profiles in order to perform type of service (ToS) overwrite by enabling a default ToS overwrite to be bound to all DOCSIS 1.0 Cable Modem (CM) created profiles.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Default DOCSIS 1.0 ToS Overwrite

No special equipment or software is needed to use the Default DOCSIS 1.0 ToS Overwrite feature.

Restrictions for Default DOCSIS 1.0 ToS Overwrite

- The Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS version 1.0.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will need to be reset in order for the effect to take place.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will display the default values that were configured. After which, overwrite values can only be changed by editing the QoS profiles.

Information About Default DOCSIS 1.0 ToS Overwrite

To configure the Default DOCSIS 1.0 ToS Overwrite feature, you should understand the following topic:

Default DOCSIS 1.0 ToS Overwrite Overview

Currently, ToS overwrite requires the creation of static cable QoS profiles, which are assigned ToS fields and are than associated with 1.0 CMs. This implementation works well if only a few different service types are offered.

However, scalability issues arises 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

Created by CableLabs, Data Over Cable Service Interface Specification (DOCSIS) defines the interface standards and requirements for all cable modems associated with high-speed data distribution over a cable television system network.

The DOCSIS architecture consists of the following two components:

- Cable Modem (CM)
- Cable Modem Termination System (CMTS)

Each of these components are situated at different locations, often with the CM located on a customer site and the CMTS on the service provider site, and communication between the CM and CMTS is conducted over cable through DOCSIS.

Note Though there are several versions of DOCSIS available, the Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS 1.0.

Type-of-Service (ToS)

Tools such as type-of-service (ToS) bits identification make it possible to isolate network traffic by the type of application being used. ToS capabilities can be further expanded to isolate network traffic down to the specific brands, by the interface used, by the user type and individual user identification, or by the site address.

How to Configure Default DOCSIS 1.0 ToS Overwrite

The tasks in this section enables the use of the Default DOCSIS 1.0 ToS Overwrite feature.

Enabling Default DOCSIS 1.0 ToS Overwrite

All CMs with a DOCSIS 1.0 configuration file currently have their ToS overwrite default values are set to tos-and: 0xff and tos-or: 0x00. Since there were previously no mechanism in the DOCSIS 1.0 configuration file to specify the ToS overwrite, QoS profiles were created and assigned to the default ToS overwrites.

The following procedures enable the Default DOCSIS 1.0 ToS Overwrite feature, which will allow a default ToS overwrite to be bound to all CM created profiles.

Before You Begin

There are no prerequisites for these procedures.

Note

- The Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS version 1.0.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will need to be reset in order for the effect to take place.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will display the default values that were configured. After which, overwrite values can only be changed by editing the QoS profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable default-tos-qos10 tos-overwrite** *tos-and tos-or* **Example:** `Router(config)# cable default-tos-qos10 tos-overwrite 0x1F 0xE0`	Configures the ToS overwrite default value for the CM. This default value will be bound to all future CM created profiles.
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

After configuring the ToS overwrite default value, reset the CM using the **clear cable modem delete** command to allow the new ToS overwrite default value to take effect.

Editing QoS Profiles

Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, additional ToS overwrite values can be changed by editing the QoS profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos profile** {*groupnum* | *ip-precedence* | *guaranteed-upstream* | *max-burst* | *max-upstream* | *max-downstream* | *priority* | *tos-overwrite* | *value*	Configures the QoS profile.

	Command or Action	Purpose
	Example: `Router(config)# cable qos profile 4 guaranteed-upstream 2`	
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Additional References

The following sections provide references related to the Default DOCSIS 1.0 ToS Overwrite feature.

Related Documents

Related Topic	Document Title
CMTS Commands	*Cisco Broadband Cable Command Reference Guide,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.3 Commands	Cisco IOS Release 12.3 Configuration Guides and Command References, at the following URL http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	To locate and download Request for Comments (RFCs) and Internet Drafts, see the Internet Engineering Task Force (IETF) web site at the following URL: http://www.ietf.org/index.html

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

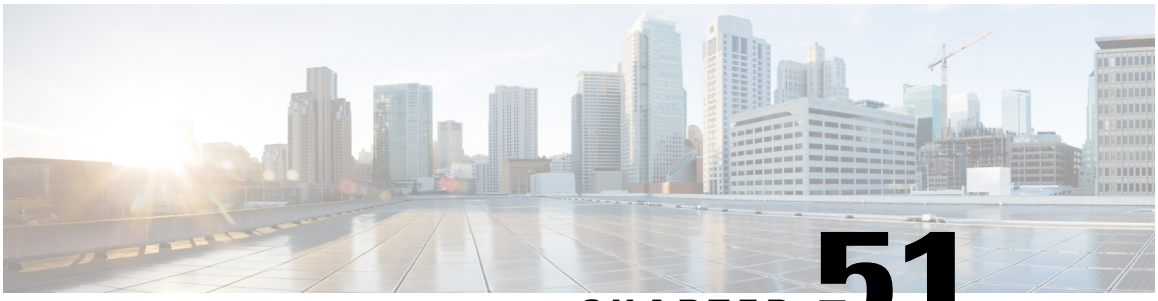
Feature Information for Default DOCSIS 1.0 ToS Overwrite

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 133: Feature Information for Default DOCSIS 1.0 ToS Overwrite

Feature Name	Releases	Feature Information
Default DOCSIS 1.0 ToS Overwrite	12.3(17a)BC2	This feature eliminates the need to create multiple QoS profiles in order to perform type of service (ToS) overwrite by enabling a default ToS overwrite to be bound to all DOCSIS 1.0 Cable Modem (CM) created profiles. The cable default-tos-qos10 tos-overwrite command was introduced by this feature.
Default DOCSIS 1.0 ToS Overwrite	12.2(33)SCD2	The priority of the QoS profile-2 is now configurable.



CHAPTER 51

DOCSIS 1.1 for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 15, 2015

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS Release12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure the Cisco CMTS router for Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 operations.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS 1.1 Operations

To support DOCSIS 1.1 operations, the CMTS must be running Cisco IOS Release 12.1(4)BC1 or later Cisco IOS Release 12.2 BC, and the cable modem must also support the DOCSIS 1.1 feature set. In addition, before you power on and configure the Cisco CMTS, check the following points:

- Ensure that your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified, based on NTSC or appropriate international cable plant recommendations. Ensure that your plant meets all DOCSIS downstream and upstream RF requirements.
- Ensure that your Cisco CMTS is installed according to the instructions provided in the appropriate Hardware Installation Guide. The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable line card to serve as the RF cable TV interface.
- Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational, based on the services to support. This includes all routers, servers (DHCP, TFTP, and ToD), network management systems, and other configuration or billing systems. This includes IP telephony equipment including gatekeepers and gateways; backbone and other equipment if supporting virtual private networks (VPNs); and dialup access servers, telephone circuits and connections and other equipment if supporting telco return.
- Ensure that DHCP and DOCSIS configuration files have been created and pushed to appropriate servers such that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TFTP and ToD server addresses, and download DOCSIS configuration files. Optionally, ensure that your servers can also download updated software images to DOCSIS 1.0 and DOCSIS 1.1 cable modems.
- Ensure that customer premises equipment (CPE)—cable modems or set-top boxes, PCs, telephones, or facsimile machines—meet the requirements for your network and service offerings.
- Familiarize yourself with your channel plan to ensure assigning of appropriate frequencies. Outline your strategies for setting up bundling or VPN solution sets, if applicable, to your headend or distribution hub. Know your dial plan if using H.323 for VoIP services and setting up VoIP-enabled cable modem configuration files. Obtain passwords, IP addresses, subnet masks, and device names, as appropriate.
- Ensure that the system clocks on the Cisco CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the Cisco CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the cable modem (CM).

After these prerequisites are met, you are ready to configure the Cisco CMTS. This includes, at a minimum, configuring a host name and password for the Cisco CMTS and configuring the Cisco CMTS to support IP over the cable plant and network backbone.

Caution If you plan to use service-class-based provisioning, the service classes must be configured at the Cisco CMTS before cable modems attempt to make a connection. Use the **cable service class** command to configure service classes.

Restrictions for DOCSIS 1.1 Operations

DOCSIS 1.1 operations includes the following restrictions:

Baseline Privacy Interface Plus Requirements

BPI+ encryption and authentication must be supported and enabled by both the cable modem and CMTS. In addition, the cable modem must contain a digital certificate that conforms to the DOCSIS 1.1 and BPI+ specifications.

Also, ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

Note Ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

BPI+-Encrypted Multicast Not Supported with Bundled Subinterfaces on the Cisco uBR10012 Router

The current Cisco IOS releases do not support using BPI+ encrypted multicast on bundled cable subinterfaces on the Cisco uBR10012 router. Encrypted multicast is supported on bundled cable interfaces or on non-bundled cable subinterfaces, but not when a subinterface is bundled on the Cisco uBR10012 router. This restriction does not apply to Cisco uBR7200 series routers.

BPI+ Not Supported with High Availability Configurations

The current Cisco IOS releases do not support using BPI+ encrypted multicast on a cable interface when the interface has also been configured for N+1 (1:n) High Availability or Remote Processor Redundancy Plus (RPR+) High Availability redundancy.

In addition, BPI+ is not automatically supported after a switchover from the Working cable interface to the Protect cable interface, because the cable interface configurations that are required for BPI+ encryption are not automatically synchronized between the two interfaces. A workaround for this is to manually configure the Protect cable interfaces with the required configurations.

Cable Interface Cards

DOCSIS 1.1 traffic is supported on Cisco uBR-MC1XC and Cisco uBR-MC28C cable interface line cards. The Cisco uBR-MC11 (FPGA) and Cisco uBR-MC16B line cards do not support DOCSIS 1.1.

Cable Privacy Hotlist CLI Not Supported on Cisco uBR10012 Router

The **cable privacy hotlist** command is not supported on the Cisco uBR10012 router running Cisco IOS releases prior to Cisco IOS release 12.3(23)BC9, Cisco IOS release 12.2(33)SCB5, and Cisco IOS release12.2(33)SCC.

To add a manufacturer's or CM certificate to the hotlist on the Cisco uBR10012 router, use SNMP commands to set the appropriate attributes in DOCS-BPI-PLUS-MIB . See the Adding a Certificate as a Trusted Certificate Using SNMP Commands, on page 1381.

DOCSIS Root Certificates

The Cisco CMTS supports only one DOCSIS Root CA certificate.

Maximum Burst Size

Previously, the maximum concatenated burst size parameter could be set to zero to specify an unlimited value. In a DOCSIS 1.1 environment, this parameter should be set to a nonzero value, with a maximum value of 1522 bytes for DOCSIS 1.0 cable modems.

If a cable modem attempts to register with a maximum concatenation burst size of zero, the DOCSIS 1.1 CMTS refuses to allow the cable modem to come online. This avoids the possibility that a DOCSIS 1.0 cable modem could interfere with voice traffic on the upstream by sending extremely large data packets. Since DOCSIS 1.0 does not support fragmentation, transmitting such data packets could result in unwanted jitter in the voice traffic.

In addition, DOCSIS 1.1 requires that the maximum transmit burst size be set to either 1522 bytes or the maximum concatenated burst size, whichever is larger. Do not set the maximum concatenation burst size to values larger than 1522 bytes for DOCSIS 1.0 cable modems.

Note This change requires you to change any DOCSIS configuration files that specify a zero value for the maximum concatenation burst size. This limitation does not exist for DOCSIS 1.1 cable modems unless fragmentation has been disabled.

Performance

DOCSIS 1.0 cable modems lack the ability to explicitly request and provide scheduling parameters for advanced DOCSIS 1.1 scheduling mechanisms, such as unsolicited grants and real-time polling. DOCSIS 1.1 cable modems on the same upstream channel can benefit from the advanced scheduling mechanisms and a DOCSIS 1.1 CMTS can still adequately support voice traffic from DOCSIS 1.1 cable modems with DOCSIS 1.0 cable modems on the same upstream channel.

Provisioning

The format and content of the TFTP configuration file for a DOCSIS 1.1 cable modem are significantly different from the file for a DOCSIS 1.0 cable modem. A dual-mode configuration file editor is used to generate a DOCSIS 1.0 style configuration file for DOCSIS 1.0 cable modems and a DOCSIS 1.1 configuration file for DOCSIS 1.1 cable modems.

Registration

A DOCSIS 1.1 CMTS must handle the existing registration Type/Length/Value parameters from DOCSIS 1.0 cable modems as well as the new type TLVs from DOCSIS 1.1 cable modems. A DOCSIS 1.0 and DOCSIS 1.1 cable modem can successfully register with the same DOCSIS 1.1 CMTS.

A DOCSIS 1.1 cable modem can be configured to make an indirect reference to a service class that has been statically defined at the CMTS instead of explicitly asking for the service class parameters. When this registration request is received by a DOCSIS 1.1 CMTS, it encodes the actual parameters of the service class in the registration response and expects a DOCSIS 1.1-specific registration-acknowledge MAC message from the cable modem.

When a DOCSIS 1.0 cable modem registers with a DOCSIS 1.1 CMTS, the registration request explicitly requests all nondefault service-class parameters in the registration. The absence of an indirect service class

reference eliminates the need for the DOCSIS 1.1 TLVs and eliminates the need to establish a local registration acknowledge wait state.

When a DOCSIS 1.1 CMTS receives a registration request from a DOCSIS 1.0 cable modem, it responds with the DOCSIS 1.0 style registration response and does not expect the cable modem to send the registration-acknowledge MAC message.

Information about DOCSIS 1.1

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.

The DOCSIS 1.1 specification provides the following feature enhancements over DOCSIS 1.0 networks:

Baseline Privacy Interface Plus

DOCSIS 1.0 introduced a Baseline Privacy Interface (BPI) to protect user data privacy across the shared-medium cable network and to prevent 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 also includes authentication, authorization, and accounting (AAA) features.

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

- X.509 Digital certificates provide secure user identification and authentication. The Cisco CMTS supports both self-signed manufacturer's certificates and certificates that are chained to the DOCSIS Root CA certificate.
- 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.
- Support for encrypted multicast broadcasts, so that only authorized service flows receive a particular multicast broadcast.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the risk of interception, interference, or alteration.

Concatenation

Concatenation allows a cable modem to make a single time-slice request for multiple upstream packets, sending all of the packets in a single large burst on the upstream. Concatenation can send multiple upstream packets as part of one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, reducing the delay in transmitting the packets on the upstream channel. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

Dynamic MAC Messages

Dynamic Service MAC messages allow the cable modem to dynamically create service flows on demand. These messages are DOCSIS link layer equivalents of the higher layer messages that create, tear down, and modify a service flow.

The DOCSIS 1.1 dynamic services state machine supports the following 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.

Note These messages are collectively known as DSX messages.

Enhanced Quality of Service

DOCSIS 1.1 provides enhanced quality of service (QoS) capabilities to give priority for real-time traffic such as voice and video:

- The DOCSIS 1.0 QoS model (a service ID (SID) associated with a QoS profile) has been replaced with a service flow and service class model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions.
- Support for multiple service flows per cable modem allows 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.
- Upstream service flows can be assigned one of the following QoS scheduling types, depending on the type of traffic and application being used:
    - Best-effort—Data traffic sent on a non-guaranteed best-effort basis. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
    - Real-time polling (rtPS)—Real-time service flows, such as video, that produce unicast, variable size packets at fixed intervals.
    - Non-real-time polling service (nrtPS)—Similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem depending on the amount of traffic and congestion on the network.
    - Unsolicited grants (UGS)—Constant bit rate (CBR) or committed information rate (CIR) traffic, such as voice, that is characterized by fixed-size packets at fixed intervals, providing a guaranteed minimum data rate.
    - 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.

Fragmentation

DOCSIS fragmentation allows the upstream MAC scheduler to slice large data requests to fit into the scheduling gaps between UGS (voice slots). This prevents large data packets from affecting real-time traffic, such as voice and video.

Fragmentation reduces the run-time jitter experienced by the UGS slots when large data grants preempt the UGS slots. Disabling fragmentation increases the run-time jitter, but also reduces the fragmentation reassembly overhead for fragmented MAC frames.

Note DOCSIS fragmentation should not be confused with the fragmentation of IP packets, which is done to fit the packets on network segments with smaller maximum transmission unit (MTU) size. DOCSIS Fragmentation is Layer 2 fragmentation that is primarily concerned with efficiently transmitting lower-priority packets without interfering with high-priority real-time traffic, such as voice calls. IP fragmentation is done at Layer 3 and is primarily intended to accommodate routers that use different maximum packet sizes.

Interoperability

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

Payload Header Suppression

Payload header suppression (PHS) conserves link-layer bandwidth by suppressing repetitive or redundant packet headers on both upstream and downstream service flows. PHS is enabled or disabled per service flow, and each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed. This ensures that PHS is done in the most efficient manner for each service flow and its particular type of application.

Downstream ToS Overwrite

Starting with Cisco IOS Release 12.2(33)SCI1, Downstream ToS Overwrite is supported in DOCSIS 1.1. It can be used in IPv4 and IPv6 environment. You can use CLI command **cable service class** *class-index* **tos-overwrite** *and-mask or-mask* or the cable modem configuration file to configure downstream ToS overwrite. For more information, see Cisco IOS CMTS Cable Command Reference Guide.

Note This feature is supported only by the Cisco uBR10012 router.

DOCSIS 1.1 Quality of Service

The DOCSIS 1.1 QoS framework is based on the following objects:

- Service flow—A unidirectional sequence of packets on the DOCSIS link. Separate service flows are used for upstream and downstream traffic, and define the QoS parameters for that traffic.

- Service class—A collection of settings maintained by the CMTS that provide a specific QoS service tier to a cable modem that has been assigned a service flow associated with that service class.
- Packet classifier—A set of packet header fields used to classify packets onto a service flow to which the classifier belongs. The CMTS uses the packet classifiers to match the packet to the appropriate service flow.
- Payload header suppression (PHS) rule—A set of packet header fields that are suppressed by the sending entity before transmitting on the link, and are restored by the receiving entity after receiving a header-suppressed frame transmission. PHS increases the bandwidth efficiency by removing repeated packet headers before transmission.

See the following sections for more information on these components.

Service Flow

In DOCSIS 1.1, the basic unit of QoS is the service flow, which is a unidirectional sequence of packets transported across the RF interface between the cable modem and CMTS. A service flow defines a set of QoS parameters such as latency, jitter, and throughput assurances, and these parameters can be applied independently to the upstream and downstream traffic flows. This is a major difference from DOCSIS 1.0 networks, where the same QoS parameters were applied to both the downstream and upstream flows.

Note DOCSIS 1.0 networks used service IDs (SIDs) to identify the QoS parameter set for a particular flow. DOCSIS 1.1 networks use the service flow ID (SFID) to identify the service flows that have been assigned to a particular upstream or downstream. DOCSIS 1.1 networks still use the term SID, but it applies exclusively to upstream service flows.

Every cable modem establishes primary service flows for the upstream and downstream directions, with a separate SFID for the upstream and the downstream flows. The primary flows maintain connectivity between the cable modem and CMTS, allowing the CMTS to send MAC management messages at all times to the cable modem.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows either can be permanently created (by configuring them in the DOCSIS configuration file that is downloaded to the cable modem), or the service flows can be created dynamically to meet the needs of the on-demand traffic, such as voice calls. Permanent service flows remain in effect, even if they are not being used, while dynamic service flows are deleted when they are no longer needed.

At any given time, a service flow might be in one of three states (provisioned, admitted, or active). Only active flows are allowed to pass traffic on the DOCSIS network. Every service flow is identified by an SFID, while upstream service flows in the admitted and active state have an extra Layer 2 SID associated with them. The SID is the identifier used by the MAC scheduler when specifying time-slot scheduling for different service flows.

Service Class

Each service flow is associated with a service class, which defines a particular class of service and its QoS characteristics, such as the maximum bandwidth for the service flow and the priority of its traffic. The service class attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified when a cable modem dynamically requests a service flow and the CMTS creates it.

The DOCSIS 1.1 service class also defines the MAC-layer scheduling type for the service flow. The schedule type defines the type of data burst requests that the cable modem can make, and how often it can make those requests. The following types of schedule types are supported:

- Best-effort (BE)—A cable modem competes with the other cable modems in making bandwidth requests and must wait for the CMTS to grant those requests before transmitting data. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
- Real-time polling service (rtPS)—A cable modem is given a periodic time slot in which it can make bandwidth requests without competing with other cable modems. This allows real-time transmissions with data bursts of varying length.
- Non-real-time polling service (nrtPS)—A cable modem is given regular opportunities to make bandwidth requests for data bursts of varying size. This type of flow is similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem, depending on the amount of traffic and congestion on the network.
- Unsolicited grant service (UGS)—A cable modem can transmit fixed data bursts at a guaranteed minimum data rate and with a guaranteed maximum level of jitter. This type of service flow is suitable for traffic that requires a Committed Information Rate (CIR), such as Voice-over-IP (VoIP) calls.
- Unsolicited grant service with activity detection (UGS-AD)—Similar to the UGS type, except that the CMTS monitors the traffic to detect when the cable modem is not using the service flow (such as voice calls when nobody is speaking). When the CMTS detects silence on the service flow, the CMTS temporarily switches the service flow to an rtPS type. When the cable modem begins using the flow again, the CMTS switches the flow back to the UGS type. This allows the CMTS to more efficiently support VoIP calls.

Each service flow is assigned a single service class, but the same service class can be assigned to multiple service flows. Also, a cable modem can be assigned multiple service flows, allowing it to have multiple traffic flows that use different service classes.

Packet Classifiers

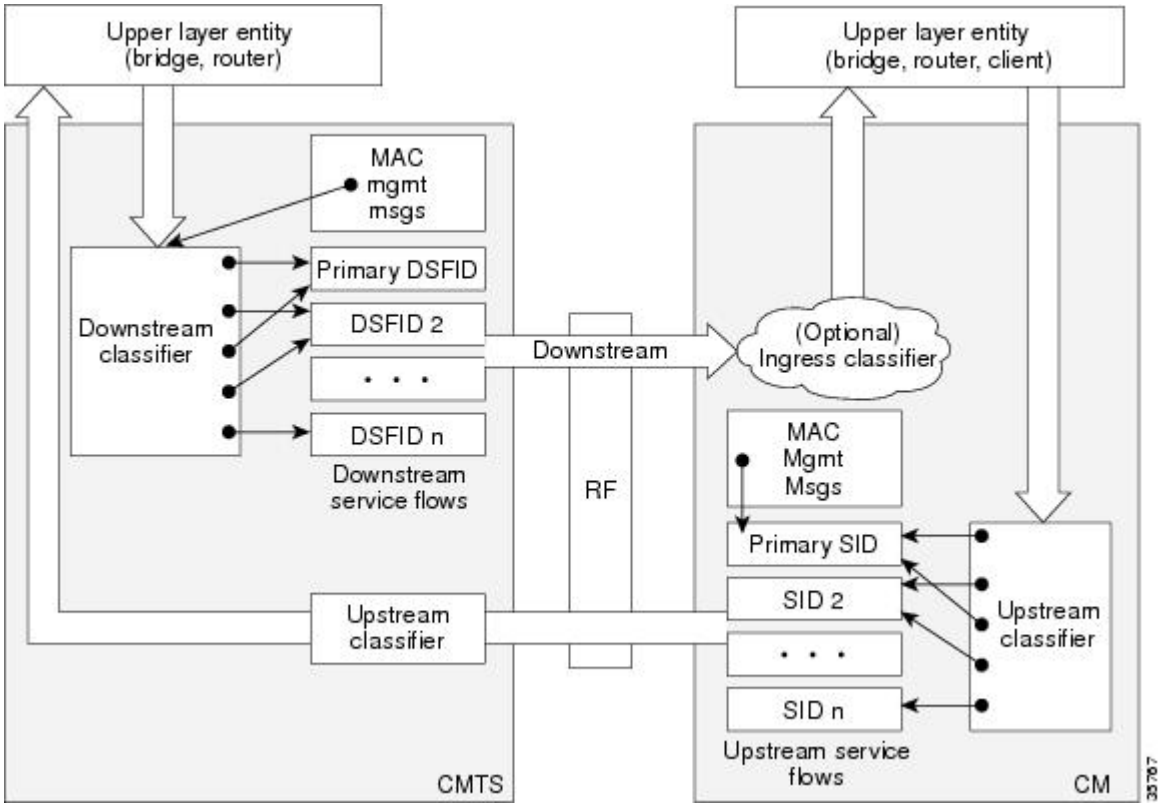
In DOCSIS 1.0 networks, a cable modem used only one set of QoS parameters for all of its traffic, so the CMTS simply had to route packets to and from the appropriate cable modems. In DOCSIS 1.1 networks, however, cable modems can be using multiple service flows, and each service flow can be given a different level of service. To quickly assign upstream and downstream packets to their proper service flows, the CMTS uses the concept of packet classifiers.

Each packet classifier specifies one or more packet header attributes, such as source MAC address, destination IP address, or protocol type. The classifier also specifies the service flow to be used when a packet matches this particular combination of headers. Separate classifiers are used for downstream and upstream service flows.

When the CMTS receives downstream and upstream packets, it compares each packet's headers to the contents of each packet classifier. When the CMTS matches the packet to a classifier, the CMTS then assigns the proper SFID to the packet and transmits the packet to or from the cable modem. This ensures that the packet is assigned its proper service flow, and thus its proper QoS parameters.

Figure below illustrates the mapping of packet classifiers.

Figure 31: Classification Within the MAC Layer



Packet Header Suppression Rules

Because many data and real-time applications may use fixed values in their packet header fields, DOCSIS 1.1 supports PHS to suppress the duplicate portions of the packet headers when a group of packets is transmitted during a session. Each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed.

When PHS is being used, the transmitting CMTS suppresses the specified headers in all the packets for that service flow. The receiving CMTS then restores the missing headers before forwarding the packets on to their ultimate destination.

Proper use of PHS can increase the efficiency of packetized transmissions, especially for real-time data that is encapsulated by other protocols, such as VoIP traffic.

Quality of Service Comparison

This section summarizes the differences in QoS between DOCSIS 1.0, DOCSIS 1.0+, and DOCSIS 1.1 networks.

Note Cisco CMTS routers running Cisco IOS Release 12.1(4)CX or later can transparently interoperate with cable modems running DOCSIS 1.0, DOCSIS 1.0+ extensions, or DOCSIS 1.1. If a cable modem indicates at system initialization that it is DOCSIS 1.1-capable, the Cisco CMTS router uses the DOCSIS 1.1 features. If the cable modem is not DOCSIS 1.1-capable, but does support the DOCSIS 1.0+ QoS extensions (for example, a Cisco uBR924 cable access router running Cisco IOS Release 12.1(1)T or later release), the Cisco CMTS automatically supports the cable modem's requests for dynamic services. Otherwise, the cable modem is treated as a DOCSIS 1.0 device.

DOCSIS 1.0

DOCSIS1.0 uses a static QoS model that is based on a class of service (CoS) that is preprovisioned in the DOCSIS configuration file that is downloaded to the cable modem. The CoS is a bidirectional QoS profile that applies to both the upstream and downstream directions, and that has limited control, such as peak rate limits in either direction, and relative priority on the upstream.

DOCSIS 1.0 defines the concept of a service identifier (SID), which identifies the cable modems that are allowed to transmit on the network. In DOCSIS 1.0 networks, each cable modem is assigned only one SID for both the upstream and downstream directions, creating a one-to-one correspondence between a cable modem and its SID. All traffic originating from, or destined for, a cable modem is mapped to that particular SID.

Typically, a DOCSIS 1.0 cable modem has one CoS and treats all traffic the same, which means that data traffic on a cable modem can interfere with the quality of a voice call in progress. The CMTS, however, has a limited ability to prioritize downstream traffic based on IP precedent type-of-service (ToS) bits.

For example, voice calls using higher IP precedence bits receive a higher queueing priority (but without a guaranteed bandwidth or rate of service). A DOCSIS 1.0 cable modem could increase voice call quality by permanently reserving bandwidth for voice calls, but then that bandwidth would be wasted whenever a voice call is not in progress.

DOCSIS 1.0+

In response to the limitations of DOCSIS 1.0 networks 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. In particular, the DOCSIS 1.0+ enhancements provide basic Voice-over-IP (VoIP) service over the DOCSIS link.

Cisco's DOCSIS 1.0+ extensions include the following DOCSIS 1.1 features:

- Multiple SIDs per cable modem, creating 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.
- 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 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.
- Unsolicited grant service (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 uBR925 cable access router.
- 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.

- 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 universal broadband router) that supports these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 cable modems continue to receive DOCSIS 1.0 treatment from the CMTS.

Interoperability with Different Versions of DOCSIS Networks

DOCSIS 1.1 cable modems have additional features and better performance than earlier DOCSIS 1.0 and 1.0+ models, but all three models can coexist in the same network. DOCSIS 1.0 and 1.0+ cable modems will not hamper the performance of a DOCSIS 1.1 CMTS, nor will they interfere with operation of DOCSIS 1.1 features.

Table below shows the interoperability of a DOCSIS 1.1 CMTS with different versions of cable modems.

Table 134: DOCSIS 1.1 Interoperability

For this configuration...	The result is...
DOCSIS 1.1 CMTS with DOCSIS 1.0 cable modems	DOCSIS 1.0 cable modems receive DOCSIS 1.0 features and capabilities. BPI is supported if available and enabled on the CMTS.
DOCSIS 1.1 CMTS with DOCSIS 1.0+ cable modems	DOCSIS 1.0+ cable modems receive basic DOCSIS 1.0 support. BPI is supported if available and enabled on the CMTS. In addition, DOCSIS 1.0+ cable modems also receive the following DOCSIS 1.1 features: • Multiple SIDs per cable modem • Dynamic service MAC messaging initiated by the cable modem • Unsolicited grant service (UGS, CBR-scheduling) on the upstream • Separate downstream rates for any given cable modem, based on the IP-precedence value • Concatenation
DOCSIS 1.1 CMTS with DOCSIS 1.1 cable modems	DOCSIS 1.1 cable modems receive all the DOCSIS 1.1 features listed in this document. BPI+ is supported if available and enabled on the CMTS.

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 on the Cisco uBR7246VXR router. Cisco IOS release 12.3(21)BC extends this support to the Cisco uBR10012 router with Performance Routing Engine 2 modules. To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the cable qos promax-ds-burst command in global configuration mode.

The ERBA feature in Cisco IOS release 12.3(21)BC is characterized by the following enhancements:

- Enables support for the DOCSIS1.1 Downstream Maximum Transmit Burst parameter on the Cisco CMTS by using the **cable ds-max-burst** configuration command. This command is not required on the Cisco uBR7225VXR, Cisco uBR7246VXR and the Cisco uBR7100 Series routers, as this parameter is supported by default.
- Allows DOCSIS1.0 modems to support the DOCSIS1.1 Downstream Maximum Transmit Burst parameter by mapping DOCSIS1.0 modems to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS.

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 allows you 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:

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

DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA

The downstream peak traffic rate TLV (DOCSIS 3.0 TLV 25.27) support for the ERBA feature was introduced in Cisco IOS Release 12.2(33)SCB1 for the Cisco uBR10012 router. This feature support was extended to Cisco uBR7246VXR and Cisco uBR7225VXR routers in Cisco IOS Release 12.2(33)SCD.

The DOCSIS WFQ Scheduler allows each service flow to have one dedicated queue. When ERBA is enabled for the service flow, the peak rate is implemented as the queue shape rate within the scheduler, while the maximum sustained rate is set as the token bucket refill rate. When ERBA is turned off, the burst size and the peak rate value are not used.

The maximum traffic burst parameter is used to control a service flow burst duration, to burst up to the channel line rate or a configured peak rate, when it is within its maximum burst size allowance. On the Cisco uBR10012 Universal Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

In Cisco IOS Release 12.2(33)SCB1, the *peak-rate* keyword was introduced to specify the peak rate an ERBA-enabled service flow can use. The peak rate value is a global value and is applied to all service flows created after the configuration of the **cable ds-max-burst** command.

If the DOCSIS 3.0 TLV 25.27 is specified for a service flow, the *peak rate* value is set as the TLV value. However, if ERBA is not turned on for a service flow, the *peak rate* value is ignored.

The *peak rate* value can also be configured using the cable service class command, which forms part of the service class template. During modem registration or Dynamic Service Addition (DSA) operation, the service class name TLV 25.4 is sent to create the static or dynamic downstream service flow that matches the service class template. These downstream service flows are created with a specific *peak rate* . If the *peak rate* is not specified, then the value specified by the **cable ds-max-burst** command is used.

If a service flow has both service class and TLV 25.27 defined *peak rate* , then the *peak rate* value specified in the TLV is used.

Some of the DOCSIS 1.x an DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when the downstream peak rate TLV 25.27 is received from the CMTS during registration. To overcome this failure, you can configure the cable service attribute withhold-TLVs command to restrict sending of the peak traffic rate TLVs to DOCSIS1.x and DOCSIS 2.0 cable modems. For more information on how to suppress peak rate TLVs, see Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems, on page 1371.

Note The ERBA feature is not applicable for high priority service flows and multicast service flows.

Table below summarizes the ERBA support for the Cisco uBR10012 router.

Table 135: Enhanced Rate Bandwidth Allocation Support for the Cisco uBR10012 Router

	Policer Rate	Policer Exceed Action	Policer Token Bucket Size	Queue Shape Rate
Traditional Service Flow	Maximum Sustained Traffic Rate (unused)	Transmit	A value computed internally by CMTS (unused)	Maximum Sustained Traffic Rate
ERBA-Enabled Service Flow	Maximum Sustained Traffic Rate	Drop	Maximum Traffic Burst TLV	Peak Traffic Rate

In Cisco uBR7246VXR and Cisco uBR7225VXR routers, the dual token bucket-based shaper is used to support ERBA on the Cisco uBR-MC88V line card (the ERBA feature is always enabled on the Cisco uBR-MC88V line card). The dual token bucket shaper has two independent token buckets for each service flow. The maximum rate of one bucket is configured to MSR and the maximum tokens are set to maximum traffic burst. The other bucket is configured with the refilling rate of the *peak rate* and the maximum tokens are set to the default level of 4 milliseconds. Packets are shaped if any of the two buckets are exhausted.

Table below summarizes the ERBA dual token bucket configuration for the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Table 136: ERBA Dual Token Bucket Configuration

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
Traditional Service Flow	Maximum Sustained Traffic Rate	4ms * MSR	N/A	N/A

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
ERBA-enabled Service Flow	Maximum Sustained Traffic Rate	Maximum Traffic Burst or 4ms * MSR	Peak Rate	4ms * Peak Rate

Note The **cable ds-max-burst** command is not supported on the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems

The DOCSIS 3.0 upstream (US) peak rate TLV 24.27 and downstream (DS) peak rate TLV 25.27 are enabled on the Cisco CMTS through the cable service class command or the CM configuration file. The DOCSIS 1.x and DOCSIS 2.0 CMs do not support these TLVs. Ideally, if a DOCSIS 1.x or DOCSIS 2.0 CM receives peak rate TLVs during registration, it should ignore these TLVs and proceed with the registration. However there are a few old non-compliant pre DOCSIS 3.0 CMs, which may fail to come online when peak-rate TLVs are received in the registration response from the Cisco CMTS. To overcome this, the Cisco CMTS enables suppression of the DOCSIS 3.0 peak rate TLVs for the pre-DOCSIS3.0 CMs.

To suppress the DOCSIS 3.0 US and DS peak rate TLVs, use the **cable service attribute withhold-TLVs command with the peak-rate** keyword in global configuration mode. When configured, this command restricts the Cisco CMTS from sending US and DS peak rate TLVs to the DOCSIS 1.x and DOCSIS 2.0 CMs. The decision to send the TLVs is based on the DOCSIS version of the CM received during registration. If the registration request is from a pre DOCSIS 3.0 CM, the peak rate TLVs are not sent in the registration response. However this command does not restrict sending of DOCSIS 3.0 peak-rate TLVs to DOCSIS 3.0 CMs.

For more information on the **cable service attribute withhold-TLVs** command, see Cisco IOS CMTS Cable Command Reference Guide .

Downstream Classification Enhancement with MAC Addresses

Downstream classifiers, specified in the cable modem configuration file, are used to map packets to service flows based on DOCSIS specifications. New combinations of downstream classifiers with a destination MAC address are supported in Cisco IOS Release 12.2(33)SCH and later. This enhancement enables service providers to better manage high priority service flows associated with a downstream classifier. For example, a single User Datagram Protocol (UDP) port can be shared by high priority and low priority traffic.

Downstream classification is automatically enabled on the Cisco CMTS router. Table below lists the downstream classifier combinations that are supported on the router.

Table 137: Downstream Classifier Combinations

Cisco IOS Release 12.2(33)SCG and Earlier	Cisco IOS Release 12.2(33)SCH and Later
Without Combination • IPv4 • IPv6 • TCP/UDP • Destination MAC With Combination • IPv4 + TCP/UDP • IPv6 + TCP/UDP	Without Combination • IP (IPv4) • IPv6 • TCP/UDP • Destination MAC With Combination • IPv4 + TCP/UDP • IPv6 + TCP/UDP • Destination MAC + IPv4 (with the exception of a destination IP address) • Destination MAC + IPv6 (with the exception of a destination IPv6 address) • Destination MAC + TCP/UDP • Destination MAC + IPv4 + TCP/UDP (with the exception of a destination IP address) • Destination MAC + IPv6 + TCP/UDP (with the exception of a destination IPv6 address)

Benefits

DOCSIS 1.1 includes a rich set of features that provide advanced and flexible QoS capabilities for various types of traffic (voice, data, and video) over the cable network. It also provides enhanced security and authentication features.

Baseline Privacy Interface Plus Enhancement

The Plus (+) version of the Baseline Privacy Interface (BPI+) in DOCSIS 1.1 provides a set of extended services within the MAC sublayer that increase performance and system security. Digital certificates provide secure authentication for each cable modem, to prevent identity theft on the basis of MAC and IP addresses. Advanced encryption provides a secure channel between the cable modem and CMTS, and secure software download allows a service provider to upgrade the software on cable modems, without the threat of interception, interference, or alteration of the software code.

Dynamic Service Flows

The dynamic creation, modification, and deletion of service flows allows for on-demand reservation on Layer 2 bandwidth resources. The CMTS can now provide special QoS to the cable modem dynamically for the

duration of a voice call or video session, as opposed to the static provisioning and reservation of resources at the time of cable modem registration. This provides a more efficient use of the available bandwidth.

Concatenation

The cable modem concatenates multiple upstream packets into one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, as opposed to requesting a time slot for each packet. This reduces the delay in transferring the packet burst upstream.

Enhanced QoS

Extensive scheduling parameters allow the CMTS and the cable modem to communicate QoS requirements and achieve more sophisticated QoS on a per service-flow level.

Different new time-slot scheduling disciplines help in providing guaranteed delay and jitter bound on shared upstream. Activity detection helps to conserve link bandwidth by not issuing time slots for an inactive service flow. The conserved bandwidth can then be reused for other best-effort data slots.

Packet classification helps the CMTS and cable modem to isolate different types of traffic into different DOCSIS service flows. Each flow could be receiving a different QoS service from CMTS.

Fragmentation

Fragmentation splits large data packets so that they fit into the smaller time slots inbetween UGS slots. This reduces the jitter experienced by voice packets when large data packets are transmitted on the shared upstream channel and preempt the UGS slots used for voice.

Multiple Subflows per SID

This feature allows the cable modem to have multiple calls on a single hardware queue. This approach scales much better than requiring a separate SID hardware queue on the cable modem for each voice call.

Payload Header Suppression

Payload Header Suppression (PHS) allows the CMTS and cable modem to suppress repetitive or redundant portions in packet headers before transmitting on the DOCSIS link. This conserves link bandwidth, especially with types of traffic such as voice, where the header size tends to be as large as the size of the actual packet.

Service Classes

The use of the service class provides the following benefits for a DOCSIS 1.1 network:

- It allows operators to move the burden of configuring service flows from the provisioning server to the CMTS. Operators provision the modems with the service class name; the implementation of the name is configured at the CMTS. This allows operators to modify the implementation of a given service to local circumstances without changing modem provisioning. For example, some scheduling parameters might need to be set differently for two different CMTSs to provide the same service. As another example, service profiles could be changed by time of day.
- It allows CMTS vendors to provide class-based-queuing if they choose, where service flows compete within their class and classes compete with each other for bandwidth.
- It allows higher-layer protocols to create a service flow by its service class name. For example, telephony signaling might direct the cable modem to instantiate any available provisioned service flow of class G.711.

Note The service class is optional. The flow scheduling specification may always be provided in full; a service flow may belong to no service class whatsoever. CMTS implementations *may* treat such unclassed flows differently from classed flows with equivalent parameters.

How to Configure the Cisco CMTS for DOCSIS 1.1 Operations

See the following sections for the configuration tasks for DOCSIS 1.1 operations. Each task in the list is identified as either required or optional.

Note This section describes only the configuration tasks that are specific for DOCSIS 1.1 operations. For complete configuration information, see the software configuration documents listed in the Additional References, on page 1411.

Configuring Baseline Privacy Interface

BPI+ encryption is by default enabled for 56-bit DES encryption on all cable interfaces. If BPI+ encryption has been previously disabled, or if you want to reconfigure BPI+ encryption on a cable interface on the CMTS, use the following procedure.

Note If you have disabled BPI+ encryption on a cable interface, and a cable modem attempts to register on that interface using BPI+ encryption, the CMTS will reject its registration request, displaying a %UBR7200-4-SERVICE_PERMANENTLY_UNAVAILABLE error message. The **show cable modem** command will also show that this cable modem has been rejected with a MAC status of reject(c).

Before You Begin

BPI+ encryption is supported on all Cisco CMTS images that include “k1”, “k8”, or “k9” in its file name or BPI in the feature set description. All BPI images support 40-bit and 56-bit DES encryption.

By default, BPI+ encryption is enabled for 56-bit DES encryption. Also, when a cable modem is running DOCSIS 1.1 software, BPI+ encryption is enabled by default, unless the service provider has disabled it by setting the Privacy Enable field (TLV 29) in the DOCSIS configuration file to 0. Therefore, both the CMTS and cable modem are set to use BPI+ encryption when using the default configurations.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable***slot /port* **Example:** `Router(config)# interface cable 6/0` `Router(config-if)#`	Enters interface configuration mode for the cable interface line card at this particular slot.
Step 4	**cable privacy** **Example:** `Router(config-if)# cable privacy` `Router(config-if)#`	(Optional) Enables BPI+ 56-bit DES encryption on the cable interface (default).
Step 5	**cable privacy 40-bit-des** **Example:** `Router(config-if)# cable privacy 48-bit-des` `Router(config-if)#`	(Optional) Enables BPI+ 40-bit DES encryption on the cable interface. Cisco does not recommend this option for production systems because 40-bit encryption is not as secure as the 56-bit DES or 168-bit 3DES encryption algorithms.
Step 6	**cable privacyaccept-self-signed-certificate** **Example:** `Router(config-if)# cable privacy accept-self-signed-certificate` `Router(config-if)#`	(Optional) Allows cable modems to register using self-signed manufacturer certificates, as opposed to the default of allowing only manufacturer's certificates that are chained to the DOCSIS root certificate. **Caution** Use the above command sparingly, as it bypasses DOCSIS BPI+ certificates. Otherwise, self-signed certificates provide workaround registration for cable modems that are not compliant with DOCSIS BPI+ certificates. This functionality is strictly intended for troubleshooting of a short duration or in the context of additional security measures. **Note** By default, the CMTS does not accept self-signed certificates. In the default configuration, if a cable modem attempts to register with self-signed certificates, the CMTS will refuse to allow the cable modem to register.
Step 7	**cable privacy authenticate-modem** **Example:** `Router(config-if)# cable privacy authenticate-modem` `Router(config-if)#`	(Optional) Enables BPI+ encryption on the cable interface and uses the Cisco IOS Authentication, Authorization and Accounting (AAA) service together with BPI to authenticate the CMs.

	Command or Action	Purpose
Step 8	**cable privacy authorize-multicast** **Example:** `Router(config-if)# cable privacy authorize-multicast` `Router(config-if)#`	(Optional) Enables BPI+ encryption on the cable interface and uses AAA protocols to authorize all multicast stream (IGMP) join requests. **Note** If you use this command to authorize multicast streams, you must also use the **cable privacy authenticate-modem** command to enable AAA services on the cable interface.
Step 9	**cable privacy mandatory** **Example:** `Router(config-if)# cable privacy mandatory` `Router(config-if)#`	(Optional) Requires baseline privacy be active for all CMs with BPI/BPI+ enabled in the DOCSIS configuration files, else the CMs are forced to go offline. If a CM does not have BPI enabled in its DOCSIS configuration file, it will be allowed to come online without BPI.
Step 10	**cable privacy oaep-support** **Example:** `Router(config-if)# cable privacy oaep-support` `Router(config-if)#`	(Optional) Enables BPI+ encryption on the cable interface and enables Optimal Asymmetric Encryption Padding (OAEP). This option is enabled by default. Disabling this option could have a performance impact.
Step 11	**cable privacy kek** {**life-time** *seconds* } **Example:** `Router(config-if)# cable privacy kek life-time 302400` `Router(config-if)#`	(Optional) Configures the life-time values for the key encryption keys (KEKs) for BPI+ operations on all cable interfaces.
Step 12	**cable privacy tek** {**life-time** *seconds*} **Example:** `Router(config-if)# cable privacy tek life-time 86400` `Router(config-if)#`	(Optional) Configures the life-time values for the traffic encryption keys (TEKs) for BPI+ operations on all cable interfaces.
Step 13	**exit** **Example:** `Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode. **Note** Repeat steps Step 3, on page 1375 through Step 13, on page 1376 for each cable interface.
Step 14	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

What to Do Next

You can also configure the following additional timers for BPI+ operations in the DOCSIS configuration file for each cable modem. As a general rule, you do not need to specify these timers in the DOCSIS configuration file unless you have a specific reason for changing them from their default values.

Table 138: Individual Cable Modem BPI+ Timer Values

Timer	Description
Authorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a KEK for the first time.
Reauthorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new KEK because the Authorization Key (KEK) lifetime is about to expire.
Authorize Reject Wait Timeout	The amount of time a cable modem must wait before attempting to negotiate a new KEK if the CMTS rejects its first attempt to negotiate a KEK.
Operational Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a TEK for the first time.
Rekey Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new TEK because the TEK lifetime is about to expire.

Downloading the DOCSIS Root Certificate to the CMTS

DOCSIS 1.1 allows cable modems to identify themselves using a manufacturer's chained X.509 digital certificate that is chained to the DOCSIS root certificate. The DOCSIS root certificate is already installed on the bootflash of the CMTS router. However, if you want to install another root certificate, for example, the Euro-DOCSIS certificate, download the certificate and save it on the bootflash as "euro-root-cert".

Tip For more information about the DOCSIS root certificate provided by Verisign, see the information at the following URL: http://www.verisign.com/products-services/index.html

Note This document previously claimed that the Cisco CMTS supports only one root certificate. This information has changed effective with Cisco IOS Release 12.3(9a)BC. In this IOS release and later releases in the 12.3 BC train, you may load the DOCSIS root certificate and a EuroDOCSIS or PacketCable root certificate. Cisco recommends that the EuroDOCSIS PacketCable root certificates be copied into bootflash. In prior Cisco IOS Releases, with the prior limitation, EuroDOCSIS or PacketCable devices could still come online, however, if they used self-signed manufacturer's digital certificates.

To download the DOCSIS root certificate to the Cisco CMTS, which is required if any cable modems on the network are using chained certificates, use the following procedure:

Step 1 Download the DOCSIS root certificate from the DOCSIS certificate signer, Verisign. At the time of this document's printing, the DOCSIS root certificate is available for download at the following URL: http://www.verisign.com/products-services/index.html

Step 2 Verisign distributes the DOCSIS root certificate in a compressed ZIP archive file. Extract the DOCSIS root certificate from the archive and copy the certificate to a TFTP server that the CMTS can access.

Tip To avoid possible confusion with other certificates, keep the file's original filename of "CableLabs_DOCSIS.509" when saving it to the TFTP server.

Step 3 Log in to the Cisco CMTS using either a serial port connection or a Telnet connection. Enter the **enable** command and password to enter Privileged EXEC mode:

Example:

```
Router> enable

Password: <password>
Router#
```

Step 4 Use the **dir bootflash** command to verify that the bootflash has sufficient space for the DOCSIS root certificate (approximately 1,000 bytes of disk space):

Example:

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  ubr7200-boot-mz.122-11.BC2.bin
3407872 bytes total (250824 bytes free)
Router#
```

Tip If you delete files from the bootflash to make room for the DOCSIS root certificate, remember to use the **squeeze** command to reclaim the free space from the deleted files.

Step 5 Use the **copy tftp bootflash** command to copy the DOCSIS root certificate to the router's bootflash memory. (The file must be named "root-cert" on the bootflash for the CMTS to recognize it as the root certificate.)

Example:

```
Router# copy tftp bootflash:

Address or name of remote host []? tftp-server-ip-address

Source filename []? CableLabs_DOCSIS.509

Destination filename [CableLabs_DOCSIS.509]? root-cert
```

```
Loading CableLabs_DOCSIS.509 from tftp-server-ip-address (via FastEthernet0/0): !
[OK - 996/1024 bytes]
996 bytes copied in 4.104 secs (249 bytes/sec)
Router#
```

Tip If you are using Cisco IOS Release 12.2(4)BC1 or later software release, you can also copy the root certificate to a PCMCIA Flash Disk (disk0 or disk1). However, because Flash Disks are not secure and easily removed from the router, we recommend that you keep the root certificate in the bootflash for both operational and security reasons.

Step 6 Verify that the DOCSIS root certificate has been successfully copied to the bootflash memory:

Example:

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  ubr7200-boot-mz.122-11.BC2.bin
    2  -rw-         996   Mar 06 2002 16:03:46  root-cert
3408876 bytes total (248696 zxbytes free)
Router#
```

Step 7 (Optional) After the first cable modem has registered using BPI+, you can use the **show crypto ca trustpoints** command to display the Root certificate that the CMTS has learned:

Note The **show crypto ca trustpoints** command does not display the root certificate until after at least one cable modem has registered with the CMTS using BPI+ encryption. Alternatively, you can use the unsupported command **test cable generate** in privileged EXEC mode to force the CMTS to register the root certificate.

Example:

```
Router# show crypto ca trustpoints
Root certificate
  Status: Available
  Certificate Serial Number: D54BB68FE934324F6B8FD0E41A65D867
  Key Usage: General Purpose
  Issuer:
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Subject Name:
    CN = "BPI Cable Modem Root Certificate Authority "
     OU = DOCSIS
     O = BPI
     C = US
  Validity Date:
    start date: 07:00:00 UTC Mar 27 2001
    end   date: 06:59:59 UTC Jan 1 2007
```

What to Do Next

Tip To display all certificates (Root, Manufacturers, CM) that the CMTS has learned, use the **show crypto ca certificates** command.

Adding a Manufacturer's Certificate as a Trusted Certificate

To DOCSIS specifications allow operators to control which manufacturer's and CM certificates are allowed on each CMTS by marking them as either trusted or untrusted. You can add a certificate to the list of trusted certificates on the Cisco CMTS using either CLI commands or SNMP commands, as described in the following sections:

Note Unless you cannot use SNMP to configure the cable modem, or have a particular application that requires the use of CLI commands to add certificates, you should also use the SNMP method to add certificates to a cable modem.

Adding a Certificate as a Trusted Certificate Using the Command Line Interface

To add a manufacturer's certificate to the list of trusted certificates on the CMTS, use the following procedure:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**cable privacy add-certificate manufacturer** *serial-number* **Example:** `Router(config)# cable privacy add-certificate manufacturer 000102` `Router(config)#`	(Optional) Specifies the serial number of the manufacturer CA certificate to be added as a trusted certificate.
Step 4	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Adding a Certificate as a Trusted Certificate Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the CMTS list of trusted certificates by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. Specify 1 for certificates that should be trusted and 3 for chained certificates that should be verified with the root certificate.

Similarly, to add a CM certificate to the list of trusted certificates, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. Specify 1 for CM certificates that should be trusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the list of trusted certificates on the CMTS at IP address 192.168.100.134, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 1
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 1
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Note If you are adding self-signed certificates, you must also use the **cable privacy accept-self-signed-certificate** command before the CMTS will accept the certificates.

Adding a Manufacturer's or CM Certificate to the Hotlist

The DOCSIS specifications allow operators to add a digital manufacturer's or CM certificate to a hotlist (also known as the certificate revocation list, or CRL) on the CMTS, to indicate that this particular certificate should no longer be accepted. This might be done when a user reports that their cable modem has been stolen, or when the service provider decides not to support a particular manufacturer's brand of cable modems.

You can add a certificate to the hotlist on the Cisco CMTS using either CLI commands or SNMP commands, as described in the following sections:

Note Unless you cannot use SNMP to configure the cable modem, or have a particular application that requires the use of CLI commands to add certificates, you should also use the SNMP method to add certificates to a cable modem.

Adding a Certificate to the Hotlist Using the Command Line Interface

To add a manufacturer's or CM certificate to the certificate hotlist on a Cisco uBR7100 series or Cisco uBR7200 series router, use the following procedure.

This procedure is not supported on the Cisco uBR10012 router running Cisco IOS releases prior to Cisco IOS release 12.3(23)BC9, Cisco IOS release 12.2(33)SCB5, and Cisco IOS Release12.2(33)SCC and later releases.

Use the following section, Adding a Certificate to the Hotlist Using SNMP Commands, on page 1384, to add certificates to the hotlist on the Cisco uBR10012 router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**cable privacy hotlist manufacturer***certificate-serial-number* **Example:** `Router(config)# cable privacy hotlist manufacturer 010A0BC304DFEE1CA98371` `Router(config)#`	Sets the trust state of the specified CA certificate to "Untrusted." Ensure that this certificate exists on the CMTS. The *certificate-serial-number* is the serial number of the CA certificate. This is not a persistent command.
Step 4	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

What to Do Next

Cable modems that use a MAC address or a certificate of the manufacturer that matches the one in the hotlist will not be allowed to register. For example, the following command will put the certificate of the manufacturer with the indicated serial number in the hotlist, preventing any cable modem that uses that certificate from registering:

```
Router# config terminal

Router(config)# cable privacy hotlist cm 00 00 0C 0a 0b 0c

Oct 31 13:06:29.112:  Successfully added CM hotlist 0000.0C0A.0B0C
Router#
```

The following command will put the manufacturer's certificate with the indicated serial number in the hotlist, preventing any cable modem that uses that manufacturer's certificate from registering:

```
Router(config)# cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01

Oct 31 13:06:34.478:  Successfully added MFG hotlist 00 90 83 00 00 00 00 01
Router(config)# exit

Router#
```

To remove a cable modem or certificate from the hotlist, add the **no** prefix to the command. For example:

```
Router# config terminal

Router(config)# no cable privacy hotlist cm 00 00 0C 0a 0b 0c

Router(config)# no cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01

Router(config)# exit
```

```
Router#
```

Adding a Certificate to the Hotlist Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the hotlist by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Similarly, to add a CM certificate to the hotlist, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

Note This procedure is identical to the one given for adding a certificate as a trusted certificate in the Adding a Certificate as a Trusted Certificate Using SNMP Commands, on page 1381, except that the docsBpi2CmtsProvisionedCmCertTrust attribute is set to 2 instead of 1.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the hotlist on the CMTS at IP address 192.168.100.113, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 2
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsProvisionedCmCertStatus.
```

```
<index>
 -i 4
 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 2
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Enabling Concatenation

To enable concatenation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable***slot* / *port* **Example:** `Router(config)# interface cable 6/0` `Router(config-if)#`	Enters interface configuration mode for the cable interface line card at this particular slot.
Step 4	**cable upstream** *n* **concatenation** **Example:** `Router(config-if)# cable upstream 0 concatenation` `Router(config-if)# cable upstream 1 concatenation` `Router(config-if)#`	Enables concatenation for the specified upstream on the cable interface. **Note** Repeat this command for each upstream on the interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

Enabling DOCSIS Fragmentation

To enable DOCSIS fragmentation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable***slot* /*port*
4. **cable upstream***n* **fragmentation**
5. **cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter* | **cac-enforce**]
6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable***slot* /*port* **Example:** `Router(config)# interface cable 6/0` `Router(config-if)#`	Enters interface configuration mode for the cable interface line card at this particular slot.
Step 4	**cable upstream***n* **fragmentation** **Example:** `Router(config-if)# cable upstream 2 fragmentation` `Router(config-if)# cable upstream 3 fragmentation` `Router(config-if)#`	Enables fragmentation for the specified upstream on the cable interface. **Note** Repeat this command for each upstream on the interface.
Step 5	**cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter* | **cac-enforce**] **Example:** `Router(config-if)# cable upstream 0 unfrag-slot-jitter limit 2000 cac-enforce` `Router(config-if)#`	(Optional) Specifies the amount of jitter that can be tolerated on the upstream due to unfragmentable slots. The **limit** option specifies the allowable *jitter* limit in microseconds (0 to 4,294,967,295. The **cac-enforce** option configures the upstream so that it rejects service flows requesting jitter less than the fragmentable slot jitter. **Note** By default, *jitter* is set to a limit of 0 microseconds, and the **cac-enforce** option is enabled.
Step 6	**exit** **Example:** `Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit` `Router#`	Exits global configuration mode.

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 profile
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 profileverbose** command in privileged EXEC mode:

```
Router# show cable qos profile 10 verbose
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
```

Enabling DOCSIS 1.1 Downstream Maximum Transmit Burst on the Cisco uBR10012 Router

Perform the following steps to configure ERBA on the Cisco uBR10012 router with PRE2 or PRE4 modules and Cisco IOS Release 12.3(21)BC or Cisco IOS Release 12.2(33)SCB or later releases. This procedure and the associated commands are subject to the guidelines and restrictions cited in this document.

Restriction The **cable ds-max-burst** and related commands are supported strictly on the Cisco uBR10012 router with PRE2 or PRE4 modules and Cisco IOS Release 12.3(21)BC or Cisco IOS Release 12.2(33)SCB or later releases.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**no**] **cable ds-max-burst** [**burst-threshold** *threshold*] [**peak-rate** *peak-rate*	Enables the support for DOCSIS 1.1 downstream max burst. To remove this configuration, use the **no** form of this command.

	Command or Action	Purpose
	Example: `Router(config)# no cable ds-max-burst burst-threshold 2048 peak-rate 1000`	• **burst-threshold***threshold* —Optional keyword and value defines the burst threshold in Kbytes, with a valid range from 64 Kbyte to 2 GB. By default, this setting is 1MB. This value is used to compare with the per-service flow maximum traffic burst value as defined in DOCSIS 2.0. • **peak-rate***peak-rate* —Peak rate in kbps. The default value of peak-rate is zero, which represents the line rate. The peak-rate value is a global value and is applied to all the service flows created after the configuration of cable ds-max-burst command.
Step 4	**Ctrl^Z** **Example:** `Router(config)# Ctrl^Z` `Router#`	Returns to privileged EXEC mode.
Step 5	**show cr10k-rp cable** *slot* / *subslot* /*port* **sid service-flow ds** **Example:** `Router(config)# show cr10k-rp cable 6/1/0 sid service-flow ds`	Displays service flows on the Cisco uBR10012 router with PRE2 or PRE4, and identifies which service flows have maximum burst enabled. • *slot* —5 to 8 • *subslot* —0 or 1 • *port* —0 to 4 (depending on the cable interface)

When this feature is enabled, new service flows with burst size larger than the burst threshold are supported. However, the existing service flows are not affected.

When this feature is disabled, no new service flows are configured with the *Downstream Maximum Transmit Burst* parameter—the **cable ds-max-burst** command settings. However, the existing service flows are not affected.

The following example illustrates the **cable ds max-burst** command on the Cisco uBR10012 router in Cisco IOS Release 12.3(21)BC:

```
Router(config)# cable ds-max-burst burst-threshold 2048
```

The following example illustrates configuration of the ERBA maximum burst for the specified service flow:

```
Router# sh cr10k-rp c7/0/0 1 service-flow ds
RP SFID  LC SFID   Conform   Conform    Exceed    Exceed    Total   Total   QID
Bytes    Pkts      Bytes     Pkts       Bytes     Pkts

32781    4         538       1        0           0          538    1       279    #
32782    4         0         0        0           0          0      0       0
#: DS max burst enabled
```

The following example illustrates the **cable ds max-burst** command on the Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCB:

```
Router(config)# cable ds-max-burst burst-threshold 2048 peak-rate 1000
```

The following example illustrates configuration of the ERBA maximum burst for the specified service flow:

```
Router# sh cr10k-rp c7/0/0 1 service-flow ds
RP SFID  LC SFID  Conform    Exceed     Conform    Exceed     Total      QID
                  Xmit Pkts  Xmit Pkts  Drop Pkts  Drop Pkts  Pkts
32930    10       41         0          0          0          41         131349
Forwarding interface: Modular-Cable1/0/0:0
32931    13       0          0          0          0          0          131350
Forwarding interface: Modular-Cable1/0/0:0
```

Monitoring DOCSIS Operations

The following sections describe the commands that provide information about the DOCSIS network and its cable modems, the RF network and cable interfaces on the CMTS, and BPI+ operations.

Monitoring the DOCSIS Network

The **show cable modem** command is the primary command to display the current state of cable modems and the DOCSIS network. This command has many options that provide information on different aspects of DOCSIS operations.

Tip For a complete description of the **show cable modem** command and its options, see the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* (see Additional References, on page 1411).

Displaying the Status of Cable Modems

The following sample output from the **show cable modem** command shows a list of known cable modems and their current status.

```
Router# show cable modems

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1     0.25    938   1    Y
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online      2    -0.25   1268   0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)  13   -0.25   1920   1    Y
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 online      16   -0.50   1920   1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 online      3    -0.50   1926   1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline     4     0.50   1929   0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 online(pt)  22   -0.50   1929   1    Y
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)  61    0.00   1925   2    Y
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)  2    !0.75   1925   1    Y
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 #online     25   -0.25   1924   1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online      15   -0.75   1914   1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online      4     0.00   1917   1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 online      17   *0.25   1919   1    N
```

You can also display a particular cable modem by specifying its MAC address or IP address with the **show cable modem** command. If you specify the MAC address or IP address for a CPE device, the command will display the information for the cable modem that is associated with that device.

Note If the CPE IP address is no longer associated with a cable modem, the **show cable modem** command might not display information about the cable modem. To display the IP address of the CPE device for the cable modem, use the **clear cable host ip-address** command to clear the IP address of the modem from the router database, and then enter the **ping docsis mac-address** command, which resolves the MAC address by sending the DOCSIS ping to the CM.

```
Router# show cable modem 0010.7bb3.fcd1

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
0010.7bb3.fcd1 10.20.113.2     C5/0/U5 online      1    0.00  1624   0    yes
```

To display a list of cable modems sorted by their manufacturer, use the **vendor** option.

```
Router# show cable modem vendor

Vendor     MAC Address    I/F       MAC         Prim  RxPwr  Timing  Num BPI
                                    State       Sid   (db)   Offset  CPE Enb
Thomson    0010.9507.01db C5/1/0/U5 online      1     0.00    938   1    N
Ericsson   0080.37b8.e99b C5/1/0/U5 online      2     -0.25   1268  0    N
Cisco      0002.fdfa.12ef C6/1/0/U0 online      13    0.00    1920  1    N
Cisco      0002.fdfa.137d C6/1/0/U0 online      16    -0.50   1920  1    N
Cisco      0003.e38f.e9ab C6/1/0/U0 online      3     -0.25   1926  1    N
Cisco      0003.e3a6.7f69 C6/1/0/U0 online      15    0.50    1927  1    N
Cisco      0003.e3a6.816d C6/1/0/U0 online      4     0.00    1929  1    N
Cisco      0006.28f9.8be5 C6/1/0/U0 online      12    0.75    1922  1    N
Cisco      0001.9659.519f C6/1/1/U2 online      26    0.25    1930  1    N
Cisco      0002.b96f.fdbb C6/1/1/U2 online      29    -0.75   1929  1    N
Cisco      0002.b96f.fdf9 C6/1/1/U2 online      39    -0.50   1931  1    N
Cisco      0002.fdfa.12e9 C6/1/1/U2 online      5     -0.25   1925  1    N
Motorola   0020.4005.3f06 C7/0/0/U0 online      2     0.00    1901  1    N
Motorola   0020.4006.b010 C7/0/0/U5 online      3     0.25    1901  1    N
Cisco      0050.7302.3d83 C7/0/0/U0 online      18    -0.25   1543  1    N
Cisco      00b0.6478.ae8d C7/0/0/U5 online      44    0.50    1920  21   N
Cisco      00d0.bad3.c0cd C7/0/0/U5 online      19    0.00    1543  1    N
```

The MAC state field in each of these displays shows the current state of the cable modem:

Table 139: Descriptions for the MAC State Field

MAC State Value	Description
Registration and Provisioning Status Conditions	
init(r1)	The CM sent initial ranging.
init(r2)	The CM is ranging. The CMTS received initial ranging from the Cm and has sent RF power, timing offset, and frequency adjustments to the CM.
init(rc)	Ranging has completed.
init(d)	The DHCP request was received. This also indicates that the first IP broadcast packet has been received from the CM.

MAC State Value	Description
init(i)	The DHCP reply was received and the IP address has been assigned, but the CM has not yet replied with an IP packet.
init(o)	The CM has begun to download the option file (DOCSIS configuration file) using the Trivial File Transfer Protocol (TFTP), as specified in the DHCP response. If the CM remains in this state, it indicates that the download has failed.
init(t)	Time-of-day (TOD) exchange has started.
resetting	The CM is being reset and will shortly restart the registration process.
Non-error Status Conditions	
offline	The CM is considered offline (disconnected or powered down).
online	The CM has registered and is enabled to pass data on the network.
online(d)	The CM registered, but network access for the CM has been disabled through the DOCSIS configuration file.
online(pk)	The CM registered, BPI is enabled and KEK is assigned.
online(pt)	The CM registered, BPI is enabled and TEK is assigned. BPI encryption is now being performed.
expire(pk)	The Cm registered, BPI is enabled, KEK was assigned but has since expired.
expire(pt)	The Cm registered, BPI is enabled, TEK was assigned but has since expired.
Error Status Conditions	

MAC State Value	Description
reject(m)	The CM attempted to register but registration was refused due to a bad Message Integrity Check (MIC) value. This also could indicate that the shared secret in the DOCSIS configuration file does not match the value configured on the CMTS with the **cable shared-secret** command. In Cisco IOS Release 12.1(11b)EC1 and Cisco IOS Release 12.2(8)BC2 or later releases, this could also indicate that the **cable tftp-enforce** command has been used to require that a CM attempt a TFTP download of the DOCSIS configuration file before registering, but the CM did not do so.
reject(c)	The CM attempted to register, but registration was refused due to a a number of possible errors: • The CM attempted to register with a minimum guaranteed upstream bandwidth that would exceed the limits imposed by the **cable upstream admission-control** command. • The CM has been disabled because of a security violation. • A bad class of service (COS) value in the DOCSIS configuration file. • The CM attempted to create a new COS configuration but the CMTS is configured to not permit such changes.
reject(pk)	KEK key assignment is rejected, BPI encryption has not been established.
reject(pt)	TEK key assignment is rejected, BPI encryption has not been established.
reject(ts)	The CM attempted to register, but registration failed because the TFTP server timestamp in the CM registration request did not match the timestamp maintained by the CMTS. This might indicate that the CM attempted to register by replaying an old DOCSIS configuration file used during a prior registration attempt.
reject(ip)	The CM attempted to register, but registration failed because the IP address in the CM request did not match the IP address that the TFTP server recorded when it sent the DOCSIS configuration file to the CM. IP spoofing could be occurring.

MAC State Value	Description
reject(na)	The CM attempted to register, but registration failed because the CM did not send a Registration-Acknowledgement (REG-ACK) message in reply to the Registration-Response (REG-RSP) message sent by the CMTS. A Registration-NonAcknowledgement (REG-NACK) is assumed.

Displaying a Summary Report for the Cable Modems

The **show cable modem** command also can provide a summary report of the cable modems by using the **summary** and **total** options.

```
Router# show cable modem summary

Interface                       Cable Modem
                  Total Registered Unregistered Offline
Cable5/1/0/U5       2     2          0            0
Cable6/1/0/U0       14    13         1            0
Cable6/1/1/U2       14    14         0            0
Cable7/0/0/U0       2     2          0            0
Cable7/0/0/U5       4     3          1            1
Router# show cable modem summary total
Interface                       Cable Modem
                  Total Registered Unregistered Offline
Cable5/1/0/U5       2     2          0            0
Cable6/1/0/U0       14    13         1            0
Cable6/1/1/U2       14    14         0            0
Cable7/0/0/U0       2     2          0            0
Cable7/0/0/U5       4     3          1            1
Total:              36    34         2            1
```

You can also use the **summary** and **total** options to display information for a single interface or a range of interfaces.

```
 Router# show cable modem summary c5/0 total

Interface     Total      Active      Registered
              Modems     Modems      Modems
Cable5/0/U0   294         272         271
Cable5/0/U1   256         248         246
Cable5/0/U2   196         194         194
Total:        746         714         711
Router# show cable modem summary c6/1/1 c7/0/0 total

Interface                       Cable Modem
                  Total Registered Unregistered Offline
Cable6/1/1/U2       14    14         0            0
Cable7/0/0/U0       2     2          0            0
Cable7/0/0/U5       4     3          1            1
Total:              20    19         1            1
```

Displaying the Capabilities of the Cable Modems

To display the capabilities and current DOCSIS provisioning for cable modems, use the **mac** option.

```
Router# show cable modem mac
```

```
MAC Address    MAC          Prim  Ver     Prov    Frag  Concat PHS   Priv  DS    US
               State        Sid                                           Saids Sids
0010.64ff.e4ad online       1     DOC1.1  DOC1.0 yes   yes    yes   BPI+  0     4
0010.f025.1bd9 init(rc)     2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.9659.4447 online(pt)   3     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.9659.4461 online(pt)   4     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.64ff.e459 online       5     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0020.4089.7ed6 online       6     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3831 online(pt)   7     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3830 online(pt)   1     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0050.7366.12fb init(i)      2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.fdfa.0a35 online(pt)   3     DOC1.1  DOC1.1 yes   yes    yes   BPI+  0     4
```

To get a summary report of the cable modems and their capabilities, use the **mac** option with the **summary** and **total** options.

```
Router# show cable modem mac summary
 total

                            Cable Modem Summary
                            -------------------
                         Mac Version                    Provision Mode
Interface       Total    DOC1.1  DOC1.0   Reg/Online   DOC1.1       DOC1.0
Cable5/1/0/U5   1        0       1        1            0            1
Cable6/1/0/U0   11       0       11       8            0            8
Cable6/1/1/U2   17       1       16       15           0            15
Cable7/0/0/U0   2        0       2        1            0            1
Cable7/0/0/U5   1        0       1        0            0            0
Total:          32       1       31       25           0            25
```

Displaying Detailed Information About a Particular Cable Modem

Several options for the show cable modem command display detailed information about a particular cable modem (as identified by its MAC address). The **verbose** option displays the most comprehensive output.

```
Router# show cable modem 0010.7bb3.fcd1 verbose

MAC Address                          : 0010.7bb3.fcd1
IP Address                           : 10.20.113.2
Prim Sid                             : 1
Interface                            : C5/0/U5
Upstream Power                       : 0 dBmV (SNR = 33.25 dBmV)
Downstream Power                     : 0 dBmV (SNR = ----- dBmV)
Timing Offset                        : 1624
Received Power                       :   0.25
MAC Version                          : DOC1.0
Capabilities                         : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                       : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support           : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support           : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPEs                       : 0(Max CPEs = 0)
Flaps                                : 373(Jun 1  13:11:01)
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 0 aborts, 3 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 1452082 packets, 171344434 bytes
Total US Throughput                  : 0 bits/sec, 0 packets/sec
Total DS Data                        : 1452073 packets, 171343858 bytes
Total DS Throughput                  : 0 bits/sec, 0 packets/sec
```

The **connectivity** and **maintenance** options also provide information that can be useful in troubleshooting problems with a particular cable modem.

The following example shows sample output for the **maintenance** option for a particular CM:

```
Router# show cable modem 0010.7bb3.fcd1 connectivity

Prim  1st time    Times  %online     Online time           Offline time
```

```
Sid   online      Online          min     avg     max     min     avg     max
1     May 30 2000 4      99.85   48:20   11h34m  1d2h23m 00:01   00:59   03:00
Router# show cable modem 0010.7bb3.fcd1 maintenance

MAC Address    I/F         Prim  SM Exhausted          SM Aborted
                           Sid   Count Time            Count Time
0010.7bb3.fcd1 C5/0/U5     1     3     Jun 1  10:24:52 0     Jan 1  00:00:00
```

Monitoring the RF Network and Cable Interfaces

You can use the **show interface cable** command to display information about the operation of the RF network and the cable interfaces on the CMTS.

Tip For a complete description of the **show cable interface** command and its options, see the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* (see http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_1_1.html#ref_1239231).

Displaying Information About Cloned Cable Modems

To display the list of cable modems detected as cloned, use the **privacy hotlist** option with the **show interface cable** command.

The following example shows how to display the cloned cable modems on a particular cable interface:

```
Router# show interface cable 5/1/0 privacy hotlist
                          Last
MAC Address               Ranged On                Type
00a0.73b0.4c43            Oct 27 21:57:39          Permanent
001a.c3ff.d2d4            Oct 27 21:57:40          Permanent
0018.6852.7746            Never                    Permanent
000e.9bb3.b946            Never                    Permanent
```

Denying RF Access For Cable Modems

To deny radio frequency (RF) access for cable modems during ranging, use the **cable privacy hotlist cm** *mac-address* command.

The following example shows how to block cloned cable modems using their own MAC address:

```
Router(config)# cable privacy hotlist cm 00C0.0102.0304
Router(config)#
```

When an operator identifies a modem's MAC address that should not be registered on a specific CMTS, the operator can add this MAC address to the CMTS using the above command. This command ensures that the modem will not be allowed to come online on any interface on that CMTS.

Displaying Information About the Mac Scheduler

To display information about the DOCSIS MAC layer scheduler that is operating on each cable interface, use the **mac-scheduler** option with the **show cable interface** command. You can display information for all of the upstreams on an interface, or you can display information for a single upstream on an interface.

The following example shows how to display information for the second upstream (U1) on a particular cable interface:

```
Router# show interface cable 3/0 mac-scheduler 1

     DOCSIS 1.1 MAC scheduler for Cable3/0/U1
     Queue[Rng Polls] 0/64, 0 drops
     Queue[CIR Grants] 0/64, 0 drops
     Queue[BE(7) Grants] 0/64, 0 drops
     Queue[BE(6) Grants] 0/64, 0 drops
     Queue[BE(5) Grants] 0/64, 0 drops
     Queue[BE(4) Grants] 0/64, 0 drops
     Queue[BE(3) Grants] 0/64, 0 drops
     Queue[BE(2) Grants] 0/64, 0 drops
     Queue[BE(1) Grants] 0/64, 0 drops
     Queue[BE(0) Grants] 0/64, 0 drops
     Req Slots 81256509, Req/Data Slots 0
     Init Mtn Slots 568433, Stn Mtn Slots 68664
     Short Grant Slots 2261, Long Grant Slots 2064698
     Awacs Slots 0
     Fragmentation count 6
     Fragmentation test disabled
     Avg upstream channel utilization : 1%
     Avg percent contention slots : 97%
     Avg percent initial ranging slots : 2%
     Avg percent minislots lost on late MAPs : 0%
     Sched Table Adm-State: Grants 1, Reqpolls 1, Util 20%
     UGS    : 0 SIDs, Reservation-level in bps 0
     UGS-AD : 1 SIDs, Reservation-level in bps 412800
     RTPS   : 0 SIDs, Reservation-level in bps 0
     NRTPS  : Not Supported
     BE     : 8 SIDs, Reservation-level in bps 0
```

Displaying Information About QoS Parameter Sets

To display information about the DOCSIS 1.1 QoS parameter sets that have been defined on a cable interface, use the **qos paramset** option with the **show cable interface** command.

```
Router# show interface cable 3/0 qos paramset

Index Name             Dir   Sched  Prio MaxSusRate  MaxBurst    MinRsvRate
1                      US    BE     0    64000       0           0
2                      DS    BE     0    1000000     0           0
3                      US    BE     0    200000      1600        0
4                      DS    BE     0    1500000     1522        0
5                      US    BE     0    500000      1522        0
6                      US    UGS_AD
7                      DS    BE     0    2000000     1522        0
8                      US    BE     0    128000      1600        0
9                      DS    BE     0    1000000     1522        0
10                     DS    BE     0    100000      1522        50000
```

You can also display detailed information for a particular parameter set by specifying the index number for its Class of Service along with the **verbose** option.

```
Router# show interface cable 3/0 qos paramset 8 verbose

Index:                                8
Name:
Direction:                            Upstream
Minimum Packet Size                   64 bytes
Admitted QoS Timeout                  200 seconds
Active QoS Timeout                    0 seconds
Scheduling Type:                      Unsolicited Grant Service(AD)
Request/Transmission Policy:          0x1FF
Nominal Polling Interval:             10000 usecs
Tolerated Poll Jitter:                2000 usecs
Unsolicited Grant Size:               500 bytes
```

```
Nominal Grant Interval:                 10000 usecs
Tolerated Grant Jitter:                 2000 usecs
Grants per Interval:                    1
IP ToS Overwrite [AND-mask,OR-mask]:    0xFF,0x0
Parameter Presence Bitfield:            {0x0, 0x3FC000}
```

Displaying Information About Service Flows

To display the service flows and their QoS parameter sets that are configured on a cable interface, use the **service-flow** option with the **show interface cable** command.

```
Router# show interface cable 3/0 service-flow

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                           Prov  Adm  Act                    State  Time
4     N/A   0001.9659.4447   4     4    4     prim    DS     act    1d0h39m
3     1     0001.9659.4447   3     3    3     prim    US     act    1d0h39m
6     N/A   0001.64ff.e4ad   6     6    6     prim    DS     act    1d0h39m
14    N/A   0006.2854.7319   9     9    9     prim    DS     act    1d0h2m
457   N/A   0006.2854.7319   10    10   0     sec(S)  DS     adm    00:00
13    6     0006.2854.7319   7     7    7     prim    US     act    1d0h2m
456   155   0006.2854.7319   8     8    8     sec(S)  US    act    21h31m
458   156   0006.2854.7319   0     11   11    dyn(S)  US     act    00:10
16    N/A   0050.7366.12fb   4     4    4     prim    DS     act    1d0h39m
15    7     0050.7366.12fb   3     3    3     prim    US     act    1d0h39m
19    N/A   0090.9607.3831   4     4    4     prim    DS     act    1d0h39m
23    10    0090.9607.3831   3     3    3     prim    US     act    1d0h39m
```

To display the major QoS parameters for each service flow, add the **qos** option to this command.

```
Router# show interface cable 3/0 service-flow qos

Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
14    DS  act   N/A   BE     0    2000000     1522      0           8124
457   DS  adm   N/A   BE     0    100000      1522      50000       0
13    US  act   6     BE     0    500000      1522      0           0
456   US  act   155   UGS_A  0    0           1522      0           57643
19    DS  act   N/A   UGS    0    100000      1522      50000       68715
```

To display the complete QoS parameters for a particular service flow, use the **qos** and **verbose** options. You can use these options separately or together.

```
Router# show interface cable 3/0 service-flow 19 verbose

Sfid                                    : 4
Mac Address                             : 0090.9607.3831
Type                                    : Primary
Direction                               : Downstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [4, 4, 4]
Active Time                             : 21h04m
Sid                                     : N/A
Traffic Priority                        : 0
Maximum Sustained rate                  : 100000 bits/sec
Maximum Burst                           : 1522 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 130
Bytes                                   : 123096
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 68715 bits/sec, 9 packets/sec
Classifiers: NONE
Router# show interface cable 3/0 service-flow 19 qos verbose

Sfid                                    : 19
Current State                           : Active
```

```
Sid                                     : N/A
Traffic Priority                        : 0
Maximum Sustained rate                  : 100000 bits/sec
Maximum Burst                           : 1522 bytes
Mimimum Reserved rate                   : 50000 bits/sec
Minimum Packet Size                     : 100 bytes
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Maximum Latency                         : 20000 usecs
Current Throughput                      : 68715 bits/sec, 9 packets/sec
```

Displaying Information About Service IDs

To display information about Service IDs (SIDs), which are assigned to only upstreams in DOCSIS 1.1 networks, use the **sid** option with the **show interface cable** command.

```
Router# show interface cable 3/0 sid

Sid  Prim  MAC Address    IP Address      Type Age      Admin   Sched  Sfid
                                                        State   Type
1          0090.9607.3831 10.1.1.35       stat 22h26m   enable  BE     3
2          0001.9659.4447 10.1.1.36       stat 22h26m   enable  BE     5
3          0000.f025.1bd9 0.0.0.0         stat 22h26m   enable  BE     7
4          0001.64ff.e4ad 10.1.1.39       stat 22h26m   enable  BE     9
5          0006.2854.7319 10.1.1.41       stat 22h26m   enable  BE     11
6          0001.9659.4461 10.1.1.33       stat 22h26m   enable  BE     13
7          0001.64ff.e459 10.1.1.42       stat 22h26m   enable  BE     15
8    5                                    stat 22h26m   enable  UGS_AD 17
9    5                                    stat 22h26m   enable  BE     18
10         0050.7366.12fb 10.1.1.43       stat 22h26m   enable  BE     20
11         0020.4089.7ed6 10.1.1.40       stat 22h26m   enable  BE     22
12   5                                    dyn  22h26m   enable  UGS    24
13   5                                    dyn  22h26m   enable  BE     25
```

Add the **qos** option to display the major QoS parameters associated with each SID.

```
Router# show interface cable 3/0 sid qos

Sid  Pr MaxSusRate MinRsvRate Sched  Grant Grant  GPI Poll   Thrput
                              Type   Size  Intvl      Intvl
1    0  200000     0          BE     100   100000 1   100000 848
2    0  200000     0          BE     100   100000 1   100000 0
3    0  64000      0          BE     0     0      0   0      0
4    0  128000     0          BE     100   100000 1   100000 0
5    0  500000     0          BE     100   100000 1   100000 0
6    0  200000     0          BE     100   100000 1   100000 848
7    0  128000     0          BE     100   100000 1   100000 0
8    0  0          0          UGS_AD 500   10000  1   10000  3468
9    0  100000     0          BE     100   100000 1   100000 0
10   0  200000     0          BE     100   100000 1   100000 848
11   0  200000     0          BE     100   100000 1   100000 848
12   0  0          0          UGS    150   100000 1   100000 0
13   0  7000       0          BE     100   100000 1   100000 0
```

To display detailed information about a particular SID and its QoS parameters, use both the **qos** and **verbose** options.

```
Router# show interface cable 3/0 sid 1 qos verbose

Sid                                     : 1
Traffic Priority                        : 0
Maximum Sustained Rate                  : 200000 bits/sec
Maximum Burst                           : 1600 bytes
Minimum Reserved Rate                   : 0 bits/sec
Minimum Packet Size                     : 64 bytes
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Maximum Concatenated Burst              : 1600 bytes
Scheduling Type                         : Best Effort
```

```
Nominal Grant Interval                  : 100000 usecs
Tolerated Grant Jitter                  : 2000 usecs
Nominal Polling Interval                : 100000 usecs
Tolerated Polling Jitter                : 2000 usecs
Unsolicited Grant Size                  : 100 bytes
Grants per Interval                     : 1
Request/Transmission Policy             : 0x0
IP ToS Overwrite [AND-mask, OR-mask]    : 0xFF, 0x0
Current Throughput                      : 863 bits/sec, 0 packets/sec
```

Monitoring BPI+ Operations

See the following sections to monitor the state of BPI operations on the CMTS and its connected cable modems:

Displaying the Current BPI+ State of Cable Modems

To display the current BPI+ state of cable modems, use the **show cable modem** command. If used without any options, this command displays the status for cable modems on all interfaces. You can also specify a particular cable interface on the CMTS, or the IP address or MAC address for a specific cable modem:

```
Router# show cable modem
 [ip-address
 | interface
 | mac-address
```

The following display shows a typical display for cable modems on all interfaces:

```
Router# show cable modem

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
0010.7b6b.58c1 0.0.0.0         C4/0/U5 offline     5   -0.25  2285   0    yes
0010.7bed.9dc9 0.0.0.0         C4/0/U5 offline     6   -0.75  2290   0    yes
0010.7bed.9dbb 0.0.0.0         C4/0/U5 online(pt)  7    0.50  2289   0    yes
0010.7b6b.58bb 0.0.0.0         C4/0/U5 reject(pk)  8    0.00  2290   0    yes
0010.7bb3.fcd1 10.20.113.2     C5/0/U5 online(pt)  1    0.00  1624   0    yes
0010.7bb3.fcdd 0.0.0.0         C5/0/U5 online(pk)  2   -20.00 1624   0    yes
0010.7b43.aa7f 0.0.0.0         C5/0/U5 reject(pt)  3    7.25  1623   0    yes
```

The following shows a typical display for a Cisco uBR10012 router for a specific interface:

```
Router# show cable modems c7/0/0

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 offline     15    -0.75   1914  1    Y
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online(pk)  4     0.00    1917  1    Y
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 reject(pk)  17   *0.25    1919  1    Y
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)  16    0.00   !2750  1    Y
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U5 online(pt)  1     0.25    1922  0    Y
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)  2     0.00    1901  1    Y
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)  3     0.00    1901  1    Y
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)  18    -0.25   1543  1    Y
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)  44    0.25    1920  21   Y
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online(pk)  19    0.25    1543  1    Y
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online(pt)  13    0.00    1546  1    Y
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 reject(pt)  12   *0.50    1546  1    Y
```

The following shows a typical display for a particular cable modem:

```
Router# show cable modem 00C0.abcd.ef01

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
00c0.abcd.ef01 10.20.113.2     C5/0/U5 online(pt)  1    0.00  1624   0    yes
```

The MAC State column displays the current status of each cable modem. The following are the possible BPI-related values for this field:

Table 140: Possible show cable modem BPI+ States

State	Description
online	A cable modem has come online and, if configured to use BPI+, is negotiating its privacy parameters for the session. If the modem remains in this state for more than a couple of minutes, it is online but not using BPI+. Check that the cable modem is running DOCSIS-certified software and is using a DOCSIS configuration file that enables BPI+.
online(pk)	The cable modem is online and has negotiated a Key Encryption Key(KEK) with the CMTS. If BPI+ negotiation is successful, this state will be shortly followed by online(pt).
online(pt)	The cable modem is online and has negotiated a Traffic Encryption Key (TEK) with the CMTS. The BPI+ session has been established, and the cable modem is encrypting all user traffic with the CMTS using the specified privacy parameters.
reject(pk)	The cable modem failed to negotiate a KEK with the CMTS, typically because the cable modem failed authentication. Check that the cable modem is properly configured for BPI+ and is using valid digital certificates. If the CMTS requires BPI+ for registration, the cable modem will go offline and have to reregister. Check that the cable modem is properly registered in the CMTS provisioning system. **Note** If a cable modem fails BPI+ authentication, a message similar to the following appears in the CMTS log: `%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem 00c0.abcd.ef01`
reject(pt)	The cable modem failed to successfully negotiate a TEK with the CMTS. If the CMTS requires BPI+ for registration, the cable modem will have to reregister.

Displaying the BPI+ Timer Values on the CMTS

To display the values for the KEK and TEK lifetime timers on a particular cable interface, use the **show interface cable** *x/y* **privacy** [**kek** | **tek**] command. For example:

```
Router# show interface cable 4/0 privacy kek
```

```
Configured KEK lifetime value = 604800
Router# show interface cable 4/0 privacy tek

Configured TEK lifetime value = 60480
```

Displaying the Certificate List on the CMTS

Use the **show crypt ca certificates** command to display the list of known certificates on the CMTS. For example:

```
Router# show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 7DBF85DDDD8358546BB1C67A16B3D832
  Key Usage: General Purpose
  Subject Name
    Name: Cisco Systems
  Validity Date:
    start date: 00:00:00 UTC Sep 12 2001
    end   date: 23:59:59 UTC Sep 11 2021
Root certificate
  Status: Available
  Certificate Serial Number: 5853648728A44DC0335F0CDB33849C19
  Key Usage: General Purpose
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Validity Date:
    start date: 00:00:00 UTC Feb 1 2001
    end   date: 23:59:59 UTC Jan 31 2031
```

Configuration Examples for DOCSIS 1.1 Operations

This section lists the following sample configurations for DOCSIS 1.1 operations on the Cisco CMTS:

Example: DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (without BPI+)

```
version 12.2
no service pad
service timestamps log datetime localtime
service password-encryption
service udp-small-servers max-servers no-limit
!
hostname 7246VXR
!
enable password 7 030A69CE09
!
cable qos profile 8
cable qos profile 10
cable qos profile 10 grant-size 1500
cable qos profile 12 guaranteed-upstream 100000
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable timeserver
!
cable config-file disable.cm
 access-denied
 service-class 1 max-upstream 1
 service-class 1 max-downstream 1600
```

```
 cpe max 1
 timestamp
!
cable config-file platinum.cm
 service-class 1 max-upstream 128
 service-class 1 guaranteed-upstream 10
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1600
 cpe max 10
 timestamp
!
clock timezone PDT -8
clock summer-time PDT recurring
clock calendar-valid
ip subnet-zero
ip cef
ip cef accounting per-prefix
no ip finger
ip tcp synwait-time 5
no ip domain-lookup
ip host vxr 192.100.168.103
ip domain-name cisco.com
ip name-server 192.100.168.70
ip name-server 192.100.168.132
ip name-server 192.100.168.250
no ip dhcp relay information check
!
!
!
ip dhcp pool cm-platinum
network 10.10.4.0 255.255.255.0
   bootfile platinum.cm
   next-server 10.10.4.1
   default-router 10.10.4.1
   option 7 ip 10.10.4.1
   option 4 ip 10.10.4.1
   option 2 hex ffff.8f80
   lease 7 0 10
!
ip dhcp pool pcs-c4
   network 192.100.168.0 255.255.255.224
   next-server 192.100.168.1
   default-router 192.100.168.1
   dns-server 192.100.168.2
   domain-name cisco.com
   lease 7 0 10
!
!
interface Ethernet2/0
 ip address 192.100.168.4 255.255.255.192
 no ip mroute-cache
 half-duplex
!
interface Cable4/0
 ip address 192.100.168.1 255.255.255.224 secondary
 ip address 10.10.4.1 255.255.255.0
 no ip route-cache cef
 no keepalive
 cable downstream rate-limit token-bucket shaping
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 555000000
 cable upstream 0 frequency 40000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
 cable dhcp-giaddr policy
!
```

```
!
router eigrp 202
 redistribute connected
 redistribute static
 network 10.0.0.0
 network 192.100.168.0
 no auto-summary
 no eigrp log-neighbor-changes
!
router rip
 version 2
 redistribute connected
 redistribute static
 network 10.0.0.0
 network 192.100.168.0
 no auto-summary
!
ip default-gateway 192.100.168.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.100.168.1
ip route 192.100.168.0 255.255.255.0 Ethernet2/0
ip http server
ip http authentication local
!
snmp-server engineID local 00000009020000E01ED77E40
snmp-server community public RO
snmp-server community private RW
tftp-server server
 tftp-server slot0:silver.cm alias silver.cm
 !
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 speed 19200
line vty 0 4
 session-timeout 60
 login
!
ntp clock-period 17179977
ntp server 192.100.168.51
end
```

Example: DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (with BPI+)

```
version 12.2
no service pad
service password-encryption
service compress-config
!
hostname uBR7246VXR
!
logging queue-limit 100
enable password 7 03085A09
!
clock summer-time EDT recurring
clock calendar-valid
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 5
cable flap-list aging 1440
cable modem max-cpe 2
cable modulation-profile 2 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 5 91 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 2 long 8 239 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 3 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 short 8 85 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
```

```
cable modulation-profile 3 long 10 235 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 4 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 4 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 short 10 8 6 8 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 4 long 10 235 0 8 16qam scrambler 152 no-diff 160 shortened uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable logging badipsource 2000000
cable time-server
!
!
ip subnet-zero
no ip source-route
!
!
ip cef
ip domain name sampleclient.com
ip dhcp smart-relay
ip dhcp relay information option
no ip dhcp relay information check
!
crypto ca trustpoint DOCSIS-ROOT-CERT
!
crypto ca certificate chain DOCSIS-ROOT-CERT
 certificate ca 00A0730000000002
  308202B7 30820220 A0030201 02020800 A0730000 00000230 0D06092A 864886F7
  0D010105 05003081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
  05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
  132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
  70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
  4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
  686F7269 7479301E 170D3030 30353038 30373030 30305A17 0D323530 35303830
  37303030 305A3081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
  05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
  132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
  70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
  4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
  686F7269 74793081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
  818100D9 C1A4199A 47D4FFAD B43F573C D1232742 748D2C91 B89E9FE9 94277008
  FBA544C8 5CC4FE3F 754BA64B AEE5A362 32A41BFE B9FD03C2 99242D95 0508DC45
  1A007021 FEC688F9 E57D9161 DE43E4EC 29379E9E 3AEB3563 455AF3B6 2C345A31
  70F4FCF6 FB39FC6E 815F05CF EC6E618A 52562F26 098C5BE1 48FD46DE E07078A9
  DD962902 03010001 300D0609 2A864886 F70D0101 05050003 8181001B DFAF32FD
  38FF13E8 CD5063C6 4663D00A 2F3132FB 25D9F6DF 1CC67C1B 5CDB5F02 825F2DD2
  72C07A3C 7EB0B138 F217E0BA CCBCF712 19AB117E 76193E86 3E7C8532 B44228A1
  0E19643A B44D66B6 15F8F142 9ECF54F6 AFCA093E A6D59067 E3F9306C 5696BF5F
  C34999A5 5F36F368 EAFAA8DD BAD93942 8620C59C 879EB625 88C3A1
  quit
!
!
!
 key chain ubr7246-rip
 key 1
  key-string 7 0600066C594C1B4F0E574345460133
!
!
interface FastEthernet0/0
ip address 192.168.10.130 255.255.255.0
 duplex half
 tag-switching ip
 no cdp enable
!
interface Ethernet1/0
 ip address 10.10.0.1 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 no ip mroute-cache
 duplex half
 no keepalive
 no cdp enable
```

```
!
interface Ethernet1/1
 ip address 10.11.0.1 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 duplex half
 no keepalive
 no cdp enable
!
interface Ethernet2/0
 ip address 192.168.10.2 255.255.0.0
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 192.168.10.1 255.255.0.0
 duplex half
 no cdp enable
!
interface Cable3/0
 ip address 192.168.10.77 255.255.255.0
 ip mask-reply
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip route-cache flow
 ip igmp access-group 96
 no ip mroute-cache
 cable map-advance dynamic 400 1000
 cable insertion-interval automatic 25 500
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 7008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 2
 no cable upstream 1 shutdown
 cable upstream 2 frequency 10000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 13008000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 2
 no cable upstream 3 shutdown
 cable upstream 4 frequency 16000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 2
 no cable upstream 4 shutdown
 cable upstream 5 frequency 20000000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 2
 no cable upstream 5 shutdown
```

```
 cable dhcp-giaddr policy
 cable privacy accept-self-signed-certificate
 cable privacy authenticate-modem
 cable privacy authorize-multicast
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable4/0
 ip address 192.168.10.55 255.255.255.0
 ip mask-reply
 no ip redirects
 no ip proxy-arp
 ip multicast ttl-threshold 5
 ip multicast boundary 15
 ip route-cache flow
 no ip mroute-cache
 cable map-advance dynamic 400 1000
 cable insertion-interval automatic 25 500
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 3
 no cable upstream 0 shutdown
 cable upstream 1 frequency 31008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 3
 no cable upstream 1 shutdown
 cable upstream 2 frequency 32000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 3
 no cable upstream 2 shutdown
 cable upstream 3 frequency 33008000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 no cable upstream 3 shutdown
 cable upstream 4 frequency 34000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 3
 no cable upstream 4 shutdown
 cable upstream 5 frequency 35008000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 3
 no cable upstream 5 shutdown
 cable source-verify leasetimer 5
 cable dhcp-giaddr policy
 cable privacy accept-self-signed-certificate
 cable privacy authenticate-modem
 cable privacy authorize-multicast
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
router rip
 version 2
 redistribute bgp 222 metric transparent
 network 10.10.0.0
```

```
 no auto-summary
!
!
ip default-gateway 192.168.100.1
ip classless
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
 no ip http server
no ip http secure-server
!
!
!
!
snmp-server community private RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps cable
snmp-server enable traps docsis-cmts
snmp-server enable traps syslog
!
line con 0
 exec-timeout 0 0
 password 7 070C285F4D06
 stopbits 1
line vty 0 4
 session-timeout 60
 exec-timeout 0 0
 password 7 0703204E
line vty 5 15
!
scheduler allocate 4000 200
end
```

Example: DOCSIS 1.1 Configuration for Cisco uBR10012 Router (with BPI+)

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname uBR10012
!
redundancy
 main-cpu
  auto-sync standard
logging queue-limit 100
no logging buffered
no logging rate-limit
enable password my-enable-password
!
ipc cache 5000
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 3/0 1gigethernet-1
card 4/0 1oc12pos-1
card 8/0 5cable-mc520s
card 8/1 5cable-mc520s
cable flap-list insertion-time 60
cable flap-list power-adjust threshold 4
cable flap-list aging 86400
cable modem vendor 00.50.F1 TI
cable spectrum-group 2 band 11000000 16000000
cable spectrum-group 21 band 17000000 25000000
cable spectrum-group 32 shared
cable spectrum-group 32 band 5000000 42000000
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
```

```
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 23 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable qos profile 5 max-downstream 10000
cable qos profile 5 max-upstream 1000
cable qos profile 5 priority 7
cable qos profile 5 tos-overwrite 0x3  0x0
cable qos profile 5 name cm_no_priority
cable qos profile 6 max-downstream 10000
cable qos profile 6 max-upstream 5000
cable qos profile 6 priority 7
cable qos profile 6 tos-overwrite 0x3  0x0
cable qos profile 6 name qos6
cable qos profile 7 max-downstream 128
cable qos profile 7 max-upstream 128
cable qos profile 7 priority 7
cable qos profile 8 max-downstream 10000
cable qos profile 8 max-upstream 1000
cable qos profile 8 priority 3
cable qos profile 8 tos-overwrite 0x3  0x0
cable qos profile 8 name qos8
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable event syslog-server 10.10.10.131
ip subnet-zero
!
!
interface FastEthernet0/0/0
 ip address 10.10.32.21 255.255.0.0
 no cdp enable
!
interface GigabitEthernet2/0/0
 ip address 10.10.31.2 255.0.0.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
interface GigabitEthernet3/0/0
 no ip address
 ip pim sparse-mode
 no ip route-cache cef
 load-interval 30
 shutdown
 negotiation auto
 no cdp enable
!
interface POS4/0/0
 no ip address
 crc 32
 no cdp enable
 pos ais-shut
!
!
interface Cable8/0/0
 ip address 10.10.10.28 255.255.255.0
 ip helper-address 1.10.10.133
 cable bundle 2 master
```

```
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 669000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable downstream rf-power 45
 cable upstream 0 connector 0
 cable upstream 0 spectrum-group 32
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 32
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 data-backoff 0 6
 cable upstream 1 modulation-profile 23
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 spectrum-group 32
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 data-backoff 3 6
 cable upstream 2 modulation-profile 23
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 spectrum-group 32
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 no cable upstream 3 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable8/0/1
 ip address 10.10.11.121
 cable bundle 2
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream max-ports 6
 cable upstream 0 connector 4
 cable upstream 0 spectrum-group 2
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23 21
 no cable upstream 0 rate-limit
 cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
```

```
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable upstream 4 channel-width 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 21
 cable upstream 4 shutdown
 cable upstream 5 channel-width 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 21
 cable upstream 5 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
ip classless
ip http server
no ip http secure-server
!
!
no cdp run
snmp-server community public RW
snmp-server community private RW
snmp-server enable traps cable
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password my-telnet-password
 login
 length 0
!
end
```

Additional References

For additional information related to DOCSIS 1.1 operations, refer to the following references:

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
HCCP N+1 Configuration	*N+1 Redundancy for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun.html

Standards

Standards[89]	Title
SP-RFIv1.1-I08-020301	*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification*
SP-BPI+-I08-020301	*DOCSIS Baseline Privacy Interface Plus Specification*

89 Not all supported standards are listed.

MIBs

MIBs[90]	MIBs Link
• DOCS-BPI-PLUS-MIB • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-CABLE-DEVICE-TRAP-MIB • DOCS-IF-EXT-MIB • DOCS-IF-MIB (RFC 2670) • DOCS-QOS-MIB • DOCS-SUBMGT-MIB • IGMP-STD-MIB (RFC 2933)	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

90 Not all supported MIBs are listed.

RFCs

RFCs[91]	Title
RFC 2669	DOCS-CABLE-DEVICE-MIB
RFC 2670	DOCS-IF-MIB
RFC 2933	IGMP-STD-MIB

91 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DOCSIS 1.1 for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

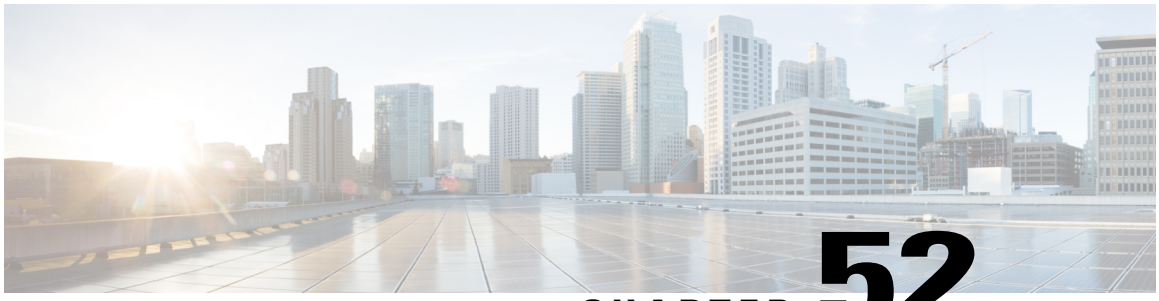
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 141: Feature Information for DOCSIS 1.1 for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 1.1 for the Cisco CMTS	12.1(4)CX	DOCSIS 1.1 support was introduced for Cisco uBR7200 series routers.
DOCSIS 1.1 for the Cisco CMTS	12.1(7)CX1	Several DOCSIS 1.1 MIBs were updated, reflecting changes in the DOCSIS 1.1 specification. The **cable submgmt default** command was also added, to set the default value of the attributes in DOCS-SUBMGT-MIB.
DOCSIS 1.1 for the Cisco CMTS	12.2(4)BC1	DOCSIS 1.1 support was introduced for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers on the Release 12.2 BC train.

Feature Name	Releases	Feature Information
N+1 redundancy	12.2(4)BC1b	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR10012 router.
N+1 redundancy	12.2(11)BC1	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR7200 series router.
UGS service flows	12.2(11)BC2	The **packetcable authorize vanilla-docsis-mta** command was supported to allow DOCSIS 1.1 cable modems to use UGS service flows when PacketCable operations have been enabled.
Enhanced Rate Bandwidth Allocation (ERBA)	12.3(13a)BC	Added support for Enhanced Rate Bandwidth Allocation (ERBA) for DOCSIS 1.0 cable modems, to include the following new configuration command and show command enhancement: • cable qos pro max-ds-burst • show cable qos profile Refer to the Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems, on page 1369.
Enhanced version of ERBA	12.3(21)BC	Added support for an enhanced version of ERBA on the Cisco uBR10012 router. Refer to the Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems, on page 1369.
DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA	12.2(33)SCB1	The ERBA feature was enhanced with the peak-rate keyword of the cable ds-max-burst command for the Cisco uBR10012 router.
DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA	12.2(33)SCD	Added support for Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Feature Name	Releases	Feature Information
Suppressing Downstream and Upstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems	12.2(33)SCB10	Support was added to restrict sending of the DOCSIS 3.0 TLVs to DOCSIS 1.X and DOCSIS 2.0 cable modems. A new command cable service attribute withhold-TLVs was introduced.
Downstream Classification Enhancement with MAC Addresses	12.2(33)SCH	New combinations of downstream classifiers with a destination MAC address are supported in Cisco IOS Release 12.2(33)SCH. For details about this feature, see Downstream Classification Enhancement with MAC Addresses, on page 1371.



CHAPTER 52

DOCSIS WFQ Scheduler on the Cisco CMTS Routers

First Published: December 18, 2008 Last Updated: July 11, 2012

Cisco IOS Release 12.2(33)SCB introduces the Data-over-Cable Service Interface Specifications (DOCSIS) Weighted Fair Queuing (WFQ) Scheduler on the Cisco uBR10012 Universal Broadband Router. The DOCSIS WFQ Scheduler is an output packet scheduler that provides output scheduling services on both WAN uplink interfaces and DOCSIS downstream interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS WFQ Scheduler

Table below shows the Cisco Cable Modem Termination System (CMTS) hardware compatibility prerequisites for this feature.

Table 142: DOCSIS 3.0 WFQ Scheduler QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V[92] Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[93]	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco Wideband SIP and Cisco Wideband SPA • Cisco 10000 Series SIP-600 and Cisco Wideband SPA or Cisco 5-Port Gigabit Ethernet SPA or Cisco 1-Port 10-Gigabit Ethernet SPA **Cisco IOS Release 12.2(33)SCH and later releases** • Cisco Next Generation Wideband SPA
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCD and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[94]	–
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCD and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[95]	–

92 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and 0 (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

93 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

94 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

95 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Note SPA interface processors (SIPs) and shared port adapters (SPAs) are required to only use DOCSIS 3.0 downstream channel bonding. Similarly, the Dynamic Bandwidth Sharing (DBS) feature is only applicable with DOCSIS 3.0 downstream channel bonding and is not a prerequisite for using the WFQ scheduler.

Restrictions for DOCSIS WFQ Scheduler

- The DBS feature is only applicable to DOCSIS 3.0 downstream channel bonding.

Information About DOCSIS WFQ Scheduler

The DOCSIS WFQ scheduling engine is used to provide output packet scheduling services, including absolute priority queueing, weighted fair queueing, minimum rate guarantee, traffic shaping, and DOCSIS bonding group dynamic bandwidth sharing on the Cisco uBR10012 universal broadband router. It replaces the existing Versatile Traffic Management System (VTMS) scheduler.

The DOCSIS WFQ Scheduler provides services on both WAN uplink interfaces and DOCSIS downstream interfaces. The scheduling parameters on WAN uplink interfaces are configured through the Modular QoS CLI (MQC). On cable downstream interfaces, queues are created for DOCSIS service flows with parameters configured by DOCSIS downstream QoS type, length, values (TLVs).

Starting with Cisco IOS Release 12.2(33)SCG, the default queue size for the DOCSIS service flows (with bandwidth greater than 150 Mbps) is increased from 255 to higher values based on the bandwidth on the cable downstream interfaces (see Table below). Additionally, the queue limit for all service flows can also be adjusted using the **cable queue-limit** command. For more information, see the Cisco IOS CMTS Cable Command Reference .

Note The default queue size change, and the **cable queue-limit** command do not affect the DOCSIS high priority queues.

Table below is an example of the queue size based on Annex B 256 QAM channels.

Table 143: Bandwidth, Queue Sizes, and Queue Limits

Channel	Bandwidth (Mbps)	Default Queue Size	Queue Size				
			1 ms	20 ms	30 ms	40 ms	200 ms
1	37.5	63	63	63	92	123	617
2	75	255	63	123	185	247	1235
3	112.5	255	63	185	277	370	1852
4	150	255	63	247	370	494	2470
5	187.5	319	63	308	463	617	3087
6	225	383	63	370	555	741	3705
7	262.5	447	63	432	648	864	4323
8	300	511	63	494	741	988	4940

Channel	Bandwidth (Mbps)	Default Queue Size	Queue Size				
			1 ms	20 ms	30 ms	40 ms	200 ms
12	450	767	63	741	1111	1482	7411
14	525	895	63	864	1296	1729	8646
16	600	1023	63	988	1482	1976	9881

For DOCSIS downstream interfaces, the DOCSIS WFQ Scheduler implements traffic shaping and physical link scheduling at two separate layers, which allows it to account for traffic overhead differently. This allows the scheduler to schedule accurately at the physical layer while conforming to DOCSIS specifications.

The DOCSIS WFQ Scheduler also allows significant enhancement to the queue scaling limits compared to the VTMS scheduler.

Table below shows the queue scaling number comparisons.

Table 144: Queue Scaling Limits

Queue Criteria	PRE4	PRE2	PRE2, Cisco IOS Release 12.2(33)SCA or earlier	NPE-G2/MC88V
Total Number of Queues Per System[96]	384,000	384,000	65,534	64,000
Total Number of CIR Queues	120,000	120,000	65,534	64,000
Number of Queues Per GE Link	16[97]	16	32[98]	N/A
Maximum Number of Packets in PXF	Small 1,703,936 Large 245,760	Small 52,428 Large 32,768	Small 52,428 Large 32,768	Small 150,000 Large 50,000
Queue Size on WAN Uplink	16,00-32,00	16,00-32,00	32,000-16,000	N/A
Queue Size on DOCSIS Downstream[99]	255	255	64	128

96 Includes network-control and default queues.

97 14 user-configurable queues, 1 class-default queue, and 1 system queue.

98 30 user-configurable queues, 1 class-default queue, and 1 system queue.

99 Starting Cisco IOS Release 12.2(33)SCG, the Queue Size on the PRE4 and PRE2 modules varies from 255 to 1023 with bandwidth 150 Mbps to 600 Mbps. See Table 2 .

The following sections explain the DOCSIS WFQ Scheduler features:

Queue Types

The DOCSIS WFQ Scheduler feature supports the following types of queues:

- Priority queues
- CIR queues
- Best Effort queues

Priority Queues

Priority queues are serviced with absolute priority over all the other queues. On DOCSIS downstream interfaces, the priority queues are configured by DOCSIS applications that request a priority service flow, for example, a packet cable voice service flow. On WAN uplink interfaces, the priority queues are configured by the MQC policy maps.

The following restrictions apply to priority queues:

- Only one priority queue is allowed per WAN uplink interface.
- Only one priority queue is allowed for low latency service flows created for each DOCSIS downstream interface.

CIR Queues

A CIR queue is guaranteed to be serviced with at least the Committed Information Rate (CIR). CIR queues are used to service DOCSIS service flows with non-zero minimum reserved rates. If the offered load to a CIR queue exceeds its CIR value, the excess traffic is serviced as best effort traffic.

The following conditions apply to CIR queues:

- CIR queues are supported only on DOCSIS downstream interfaces. They are not supported on WAN uplink interfaces.
- Each DOCSIS flow with a non-zero minimum reserved rate uses its own CIR queue.

Best Effort Queues

The Best Effort (BE) queues share the interface bandwidth not used by the priority queue and the CIR queues. The sharing is in proportion to each queue's quantum value.

The following conditions apply to BE queues:

- On DOCSIS downstream interfaces, BE queues are created by DOCSIS service flows that do not request a minimum reserved rate.
- Each DOCSIS flow without a minimum reserved rate uses its own BE queue.

DOCSIS QoS Support

DOCSIS defines a set of quality of service (QoS) parameters, including traffic priority, maximum sustained traffic rate, minimum reserved traffic rate, maximum traffic burst, maximum downstream latency, and peak traffic rate.

The downstream service flows use the QoS parameters to specify the desired QoS. The downstream policer and scheduler provides services such as traffic shaping, bandwidth provisioning, traffic prioritization, and bandwidth guarantee.

The DOCSIS service flow parameters are mapped to the packet queue parameters and provided with appropriate QoS support for the packet queues to support the DOCSIS parameters

The following DOCSIS QoS parameters are supported:

- Traffic priority
- Maximum sustained traffic rate
- Minimum reserved traffic rate

Note The maximum traffic burst size and the peak traffic rate are supported as described in the http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_wfq_scheduler.html#con_1085732.

Traffic Priority

The downstream channel bandwidth available to the best effort traffic, namely the channel bandwidth minus the amount consumed by the priority traffic and the CIR traffic, is allocated to the best effort service flows in proportion to their DOCSIS traffic priorities. For example, if there are three service flows sending packets at a particular moment over the same downstream channel, and their DOCSIS traffic priorities are 0, 1 and 3, respectively, their share of the channel bandwidth will be 1:2:4. To achieve this bandwidth allocation, each service flow is assigned a value known as its excess ratio which is derived from its DOCSIS priority. Table below shows the default mappings of DOCSIS priority to excess ratio.

Note When traffic priority for a flow is not explicitly specified, a default priority value of 0 is used as per the DOCSIS specification.

Table 145: DOCSIS Priority to Excess Ratio Mapping

DOCSIS Traffic Priority	Excess Ratio
0	4
1	8
2	12
3	16

DOCSIS Traffic Priority	Excess Ratio
4	20
5	24
6	28
7	32

Custom DOCSIS Priority to Excess Ratio Mappings

Cisco IOS Release 12.2(33)SCC introduces the option to configure custom priority to excess ratio mappings for downstream service flows that override the default mappings listed in the above Table.

Note The configured values are used only for new service flows that are created after the configuration has been applied. All the existing service flows maintain their previous excess ratio values.

The option to configure priority to excess ratio mappings is available on a per downstream forwarding interface basis and is applicable to legacy cable, wideband and modular cable, and integrated cable interfaces.

Note Modular cable interfaces are not supported on Cisco uBR7200 series routers.

The cable downstream qos wfq weights command is used to configure the mappings. For more details on this command, refer to Cisco IOS CMTS Cable Command Reference Guide .

Maximum Sustained Traffic Rate

The maximum sustained traffic rate (MSR) specifies the peak information rate of a service flow. The MSR of a service flow is mapped to the shape rate of the packet queue. When the maximum sustained traffic rate is not specified or set to zero, its traffic rate becomes limited only by the physical channel capacity set by DOCSIS specifications.

Minimum Reserved Traffic Rate

The minimum reserved traffic rate (MRR) specifies the minimum rate reserved for a service flow. The MRR of a service flow is mapped to the CIR of the packet queue, which ensures the minimum amount of bandwidth a queue gets under congestion. When the MRR is not specified, the CIR is set to zero as per DOCSIS specifications.

High Priority Traffic

High priority traffic flows are mapped to a Low Latency Queue (LLQ) on the data forwarding interface. The packets in LLQ are serviced with absolute priority over other queues on the same interface.

The following service flows require high priority service:

- Service flows with DOCSIS downstream latency TLV set to a value above zero. For example, PacketCable Multimedia Specification (PCMM) voice calls.

- PacketCable downstream service flows.
- Service flows with Unsolicited Grant Service (UGS) type—non-PacketCable voice calls—upstream flows.

Enhanced Rate Bandwidth Allocation

The DOCSIS WFQ Scheduler supports the Enhanced Rate Bandwidth Allocation (ERBA) feature for service flows. The ERBA feature allows cable modems (CMs) to burst their temporary transmission rates up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests without having to make changes to existing service levels in the QoS profile.

The DOCSIS WFQ Scheduler allows each service flow to have one dedicated queue. When ERBA is enabled for the service flow, the peak rate is implemented as the queue shape rate within the scheduler, while the maximum sustained rate is set as the token bucket refill rate. When ERBA is turned off, the burst size and the peak rate value are not used.

The maximum traffic burst parameter is used to control a service flow burst duration, to burst up to the channel line rate or a configured peak rate, when it is within its maximum burst size allowance. On the Cisco uBR10012 Universal Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

For more details on this behavior and the CLI, refer to Cisco IOS CMTS Cable Command Reference Guide .

Note The ERBA feature is not applicable for high priority service flows and multicast service flows.

Table below summarizes the ERBA support for the Cisco uBR10012 router.

Table 146: Enhanced Rate Bandwidth Allocation Support for the Cisco uBR10012 Router

	Policer Rate	Policer Exceed Action	Policer Token Bucket Size	Queue Shape Rate
Traditional Service Flow	Maximum Sustained Traffic Rate (unused)	Transmit	A value computed internally by CMTS (unused)	Maximum Sustained Traffic Rate
ERBA-Enabled Service Flow	Maximum Sustained Traffic Rate	Drop	Maximum Traffic Burst TLV	Peak Traffic Rate

In Cisco uBR7246VXR and Cisco uBR7225VXR routers, the dual token bucket-based shaper is used to support ERBA on the Cisco uBR-MC88V line card (the ERBA feature is always enabled on the Cisco uBR-MC88V line card). The dual token bucket shaper has two independent token buckets for each service flow. The maximum rate of one bucket is configured to MSR and the maximum tokens are set to maximum traffic burst. The other bucket is configured with the refilling rate of the *peak-rate* and the maximum tokens are set to the default level, of 4 milliseconds. Packets are shaped if any of the two buckets are exhausted.

Table below summarizes the ERBA dual token bucket configuration for the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Table 147: ERBA Dual Token Bucket Configuration

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
Traditional Service Flow	Maximum Sustained Traffic Rate	4ms * MSR	N/A	N/A
ERBA-enabled Service Flow	Maximum Sustained Traffic Rate	Maximum Traffic Burst or 4ms * MSR	Peak Rate	4ms * Peak Rate

For information about ERBA support on the Cisco CMTS routers, refer to Using Enhanced Bandwidth Rate Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems at the following location: DOCSIS 1.1 for the Cisco CMTS Routers

Peak Traffic Rate

Note The **cable ds-max-burst** command is not supported on the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

The *peak-rate* option of the **cable ds-max-burst** command allows you to specify the peak rate an ERBA-enabled service flow can use. The *peak-rate* value is a global value and is applied to all service flows created after the configuration of the **cable ds-max-burst** command. The default value of the *peak-rate* is zero.

If the DOCSIS 3.0 TLV 25.27 is specified for a service flow, the *peak-rate* value is set as the TLV value. However, if ERBA is not turned on for a service flow, the *peak-rate* value is ignored.

The *peak-rate* value can also be configured through cable service class command which forms part of the service class template. During modem registration or Dynamic Service Addition (DSA) operation, the service class name TLV 25.4 is sent to create the static or dynamic downstream service flow that matches the service class template. These downstream service flows are created with a specific *peak-rate* . If the *peak-rate* is not specified, then the value specified by the **cable ds-max-burst** command is used.

If a service flow has both service class and TLV 25.27 defined *peak-rate* , then the *peak-rate* value specified in the TLV is used.

Some of the DOCSIS 1.x and DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when they receive TLV 25.27 from the Cisco CMTS during registration. In order to overcome this you can configure the **cable service attribute withhold-TLVs command with the peak-rate** keyword to restrict sending of this TLV to non-DOCSIS 3.0 cable modems.

For more details on the cable service class and **cable service attribute withhold-TLVs** commands, see Cisco IOS CMTS Cable Command Reference Guide .

DOCSIS 3.0 Downstream Bonding Support with Bonding Group Dynamic Bandwidth Sharing

DOCSIS 3.0 introduces the concept of downstream channel bonding. Each Bonding Group (BG) is made up of a collection of downstream channels, which can be used by one or more bonding groups. Each downstream channel can also serve as a primary channel in a MAC domain and carry non-bonded traffic, while being part of a BG.

Prior to DOCSIS 3.0 standards, the downstream service flows were associated with a single downstream interface, which in turn corresponded to a physical downstream on an RF channel. In DOCSIS 3.0, the downstream service flows are associated with the downstream bonding groups. These bonding groups can use multiple downstream RF channels.

On the Cisco uBR10012 universal broadband router, the DOCSIS 3.0 downstream channel bonding is supported on the SPA RF channels. To efficiently utilize the underlying RF channel bandwidth and to provide QoS to the downstream service flows, dynamic bandwidth sharing (DBS) is supported on the interfaces using SPA RF channels.

DBS is the dynamic allocation of bandwidth for wideband (WB), integrated cable (IC), and modular-cable (MC) interfaces sharing the same downstream channel. Due to the channel sharing nature of the bonding groups, the bandwidth available to bonding groups or non-bonded channels is not fixed. The bandwidth depends on the configuration and the traffic load on the WB, IC, or MC.

Note Bonding groups are implemented as WB interfaces and non-bonded channels as MC interfaces.

In the DBS mode, the bandwidth of the shared RF channels is dynamically allocated among the WB, IC, and MC interfaces. The DBS enables efficient use of the underlying RF channel bandwidth even in the presence of high burst traffic. The DBS is configured at the WB, IC, or MC interface level. By default, bandwidth for a WB, IC, or MC channel is statically allocated (non-DBS).

DBS does not prevent static bandwidth configuration. If a static portion of the bandwidth is configured on any RF channel that one or more DBS-enabled channel utilizes, that portion is subtracted from the RF channel bandwidth. This portion of bandwidth is dedicated to the non-DBS interface and becomes unavailable to the DBS WB, IC, or MC interfaces.

For information about DBS support on the Cisco CMTS routers, refer to the Dynamic Bandwidth Sharing on the Cisco CMTS Router feature.

How to Configure DOCSIS WFQ Scheduler

You cannot configure the DOCSIS WFQ Scheduler feature as it is automatically loaded into the Parallel Express Forwarding (PXF) engine. The parameters that the schedule uses include the interface bandwidth and queue parameters.

This section describes the following required and optional procedures:

Mapping DOCSIS Priority to Excess Ratio

This section describes how to map DOCSIS priorities to custom excess ratios for downstream service flows. These custom mappings will override the default mappings.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*port*|*slot*/*subslot*/*port* } **Example:** `Router(config)# interface cable 3/0/0`	Enters interface configuration mode for the indicated cable downstream interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ *slot*—3 to 6 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ *slot*—1 and 2 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are: ◦ *slot* —5 to 8 ◦ *subslot* —0 or 1 ◦ *port*—0 to 4 (depending on the cable interface)
Step 4	**cable downstream qos wfq weigthts {weight1...weight8}** **Example:** `Router(config-if)# cable downstream qos wfq weights 10 20 30 40 50 60 70 80`	Configures the custom excess ratios for 8 priorities: • *weight1...weight8* —Custom weight. Valid values range from 1 to 100. **Note** The custom values are used only for new service flows and not existing ones.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Service Flows and Queues

Cisco uBR10012 Router

To verify the downstream (DS) service flows and parameters for a modem, use the **show cable modem** [**mac-address** |**ip-address**]**qos** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cable modem 0018.f826.3453 qos
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
7     US  act   1     BE     7    0           3044      0           0
8     DS  act   N/A   BE     7    0           2000000   100000      7429769
29    DS  act   N/A   BE     0    0           3044      0           0
```

To verify the detailed service flow configuration, use the **show interfaces cable-interface service-flow sfid qos** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show interfaces c7/0/0 service-flow 8 qos
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
8     DS  act   N/A   BE     7    0           2000000   100000      7430397
```

To verify the detailed service flow statistics, use the **show interfaces cable-interface service-flow sfid counters** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show interfaces c7/0/0 service-flow 8 counters
Sfid  Packets             Bytes               PacketDrop Bits/Sec   Packet/Sec
8     100913              121095600           374337     7431599    773
```

To verify the service flow ID to queue ID (queue index) association, use the **show cr10k-rp cable-interface sfid queue** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cr10k-rp mod 1/2/0:0 queue
Docsis queues on the interface: 0
Total DOCSIS Queues Allocated: 45
Available/Maximal reservable rate(kbps): 3750/3750

HQF BLT Info (LBLT Group 36):
LBLT 36: wt/qntm 1/10000; PBLT 1236: BW 3750Kbps, flowbit prd/ofst 512/0, rsrc/flrsrc 3/3

BE Queues:

CIR Queues:

LL Queues:
```

To verify the service flow queue information, use the **show pxf cpu queue interface-name** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show pxf cpu queue modular-cable 1/2/0:0
Cable Interface Queues:
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131147    0/255  190        0           0         1/240    0       58
131148    0/255  33820      0           0         1/10000  0       32824
Cable Service Flow Queues:
* Best Effort Queues
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131241    0/255  0          0           0         1/240    0       32881
* CIR Queues
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
2049    254/255  131018     485751      99        1/1920   0       32880
* Low Latency Queues
QID     Len/Max  Dequeues   TailDrops
```

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the downstream hierarchical queueing framework (HQF) queue information for a modem, use the **show cable modem [mac-address | ip-address] queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show cable modem 41.3.190.2 queue
* idx/gqid Len/Limit Deqs      Drops     CIR       MIR/PR     ForwInt  SFID
             pkts    pkts      pkts      kbps       kbps
BE Queues:
    3/43     0/128   103       0         0           0/0      In5/1:1 Ca5/1:22
CIR Queues:
Low Latency Queues:
```

To verify the downstream HQF queue information for the interface, use the **show interfaces cable-interface service-flow sfid queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue
*   idx/gqid   Len/Limit Deqs      Drops    CIR         MIR/PR
                 pkts    pkts      pkts     kbps         kbps
      0/53       0/128   0         0        100       15000/0
 I: Cable Interface Queue
 $: Low Latency Queue
 ~: Low Latency Policing Queue
```

To verify the detailed downstream HQF information for all queues under this interface, use the **show interfaces cable-interface service-flow sfid queue verbose** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue verbose
   blt (0x19FA93C0, index 6, qid 53, fast_if_number 20) layer CLASS_HIER0
   scheduling policy: FIFO (110)
   classification policy: NONE (120)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x22A208C    scheduler: 0x1A015D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1
   D/Traffic Shaping enabled
   txcount 0 txqbytes 0 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 128/375000 availbuffers 128
   holdqueue_out 0 perc 0.00 remaining_ratio/perc 20
   visible_bw 100 max_rate 15000 allocated_bw 100 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 1500, credit: 0, depth: 1500
   backpressure_policy 0 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A015D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A015D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A015D80 burst packets/bytes[NOTP] 0/0

   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 15000 increment_lower 0 increment_limit 15000
     last visit 0 credit 0 outstanding_tokens 0 maxtokens 32000000
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 562
     nextexpire_system_time 0 nextexpire_time_qindex -1
```

Verifying the DOCSIS Priority to Excess Ratio Mapping

Cisco uBR10012 Router

To verify the DOCSIS priority to excess ratio mapping configuration on the Cisco uBR10012 router, use the **show running-config interface** command as shown in the following example:

```
Router# show running-config interface cable 8/0/0 | i qos
cable downstream qos wfq weights 10 20 30 40 50 60 70 80
```

To verify the excess ratio for each queue on an interface, use the show cr10k-rp interface queue be command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cr10k cable8/1/0 queue be
Forwarding Interface: Cable8/1/0
Docsis queues on the interface: 8
Total DOCSIS Queues Allocated: 25
Available/Maximal reservable rate(kbps): 25232/26000
HQF BLT Info (LBLT Group 86):
LBLT 110: wt/qntm 1/10000; PBLT 1286: BW 26000Kbps, flowbit prd/ofst 32/3, rsrc/flrsrc 17/17

BE Queues:
Queue Index: 131268, GlobalQID 83, CBLT ID 131268
       MinRate(Kbps) 0, ExcessRatio 4, ShapeRate(bps) 10000000, QLimit 255 Service Flow(s):
 rp_sf_index 32880, lc_sfid 3, min_rate(bps) 0, max_rate(bps) 10000000 peak_rate(bps) 0
Queue Index: 131376, GlobalQID 81, CBLT ID 131376
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33115, lc_sfid 39, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131377, GlobalQID 82, CBLT ID 131377
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33116, lc_sfid 40, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
Queue Index: 131378, GlobalQID 85, CBLT ID 131378
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33120, lc_sfid 35, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131379, GlobalQID 88, CBLT ID 131379
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33121, lc_sfid 43, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
Queue Index: 131398, GlobalQID 109, CBLT ID 131398
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33170, lc_sfid 37, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131399, GlobalQID 110, CBLT ID 131399
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33171, lc_sfid 51, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
```

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the DOCSIS priority to excess ratio mapping configuration on the Cisco uBR7246VXR and Cisco uBR7225VXR routers, use the **show interfaces cable-interface service-flow sfid queue verbose** command as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue verbose
   blt (0x19FA93C0, index 6, qid 53, fast_if_number 20) layer CLASS_HIER0
   scheduling policy: FIFO (110)
   classification policy: NONE (120)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x22A208C    scheduler: 0x1A015D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1
   D/Traffic Shaping enabled
   txcount 0 txqbytes 0 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 128/375000 availbuffers 128
   holdqueue_out 0 perc 0.00 remaining_ratio/perc 20
   visible_bw 100 max_rate 15000 allocated_bw 100 vc_encap 0 ecn_threshold NONE
```

```
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 1500, credit: 0, depth: 1500
   backpressure_policy 0 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A015D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A015D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A015D80 burst packets/bytes[NOTP] 0/0

   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 15000 increment_lower 0 increment_limit 15000
     last visit 0 credit 0 outstanding_tokens 0 maxtokens 32000000
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 562
     nextexpire_system_time 0 nextexpire_time_qindex -1
```

Verifying the HQF Queue Detail Information

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the downstream HQF queue information for all the queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue
* idx/gqid Len/Limit Deqs      Drops     CIR       MIR/PR     SFID
            pkts    pkts      pkts      kbps       kbps
BE Queues:
I   0/1      0/128   0         0         0           0/0          -
    1/42     0/128   16        0         0           0/0      Ca4/0:116
    2/44     0/128   4         0         0        1000/0      Ca4/0:3890
CIR Queues:
Low Latency Queues:
 I: Cable Interface Queue
 $: Low Latency Queue
```

To verify the detailed downstream HQF queue information for all the queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue [verbose]** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 4/0:0 queue verbose
   blt (0x20265E60, index 0, qid 0, fast_if_number 20) layer PHYSICAL
   scheduling policy: WFQ (111)
   classification policy: CLASS_BASED (122)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x222000    scheduler: 0x202D2D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0
total active 0
   D/Traffic Shaping enabled
   txcount 13 txqbytes 746 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 8000/0 availbuffers 8000
   holdqueue_out 1000 perc 0.00 remaining_ratio/perc 0
   visible_bw 2600 max_rate 2600 allocated_bw 2080 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 0
   weight B 1 quantum B 1500 credit B 0
   min-rate tokens: 13000, credit: 0, depth: 13000
   backpressure_policy 1 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x202D2D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x202D2D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x202D2D80 burst packets/bytes[NOTP] 0/0
   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 2600 increment_lower 0 increment_limit 2600
```

```
     last visit 145532 credit 0 outstanding_tokens 20192 maxtokens 20800
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 21
     nextexpire_system_time 0 nextexpire_time_qindex -1
   next layer HQFLAYER_CLASS (max entries 2000)
BE Queues:
    blt (0x20265DA0, index 0, qid 1, fast_if_number 20) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    blt flags: 0x220000    scheduler: 0x202D2CC0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0
 total active 1
    txcount 13 txqbytes 746 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/0 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 0
    visible_bw 0 max_rate 26000 allocated_bw 26000 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1600 credit A 0
    weight B 1 quantum B 1600 credit B 46
    min-rate tokens: 13000, credit: 0, depth: 13000
    backpressure_policy 0 scheduler_flags C03F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x202D2CC0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x202D2CC0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x202D2CC0 burst packets/bytes[NOTP] 1/46
CIR Queues:
Low Latency Queues:
```

To verify the normal downstream HQF queue information for all the class layer bandwidth limited traffic (CBLT) queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue cblt [index | priority]** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue cblt 1
    blt (0x65CE3EA0, index 1, qid 45, fast_if_number 19) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    D/Traffic Shaping enabled
    blt flags: 0x22A208C    scheduler: 0x65D504C0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 1000 total
active 1
    D/Traffic Shaping enabled
    txcount 890 txqbytes 63900 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/100000 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 11
    visible_bw 0 max_rate 4000 allocated_bw 0 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1500 credit A 1500
    weight B 1 quantum B 1500 credit B 1500
    min-rate tokens: 1500, credit: 0, depth: 1500
    backpressure_policy 0 scheduler_flags C03F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x65D504C0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x65D504C0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x65D504C0 burst packets/bytes[NOTP] 0/0
    OUTPUT Shaping
      Bc internal 0 Be internal 0 Time interval 4
      increment 4000 increment_lower 0 increment_limit 4000
      last visit 87456736 credit 0 outstanding_tokens 23760 maxtokens 24352
      peak_rate_credit 0 peak_rate_tokens 0 peak_rate_increment 0
      system timer delayed 0 restart timer 0
      timer set 0 hqf_shape_running 17254
      nextexpire_system_time 0 nextexpire_time_qindex -1
```

To verify the normal and priority downstream HQF queue information for all the CBLT queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue cblt**

[index | priority] command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue cblt priority
    blt (0x19FA9300, index 0, qid 52, fast_if_number 20) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    blt flags: 0x200800    scheduler: 0x1A015CC0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1

    txcount 114 txqbytes 12864 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/0 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 0
    visible_bw 0 max_rate 37500 allocated_bw 0 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1500 credit A 1500
    weight B 1 quantum B 1500 credit B 1500
    min-rate tokens: 1500, credit: 0, depth: 1500
    backpressure_policy 0 scheduler_flags C83F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x1A015CC0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x1A015CC0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x1A015CC0 burst packets/bytes[NOTP] 0/0
PRIORITY LEVEL 1: total bandwidth 500 kbps, total percent 0%
```

To verify the downstream HQF queue information for all the physical layer bandwidth limited traffic (PBLT) queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue pblt** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue pblt
   blt (0x19FB4700, index 0, qid 0, fast_if_number 20) layer PHYSICAL
   scheduling policy: WFQ (111)
   classification policy: CLASS_BASED (122)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   blt flags: 0x220000    scheduler: 0x1A0210C0
  total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0 total active
 0
   txcount 67743 txqbytes 6281007 drops 2 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 8000/0 availbuffers 8000
   holdqueue_out 1000 perc 0.00 remaining_ratio/perc 0
   visible_bw 37500 max_rate 37500 allocated_bw 18000 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 13000, credit: 0, depth: 13000
   backpressure_policy 1 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A0210C0 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A0210C0 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A0210C0 burst packets/bytes[NOTP] 0/0
```

Additional References

The following sections provide references related to the DOCSIS WFQ Scheduler feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference

Related Topic	Document Title
Modular Quality of Service	MQC QoS on the Cisco CMTS Routers
Enhanced Bandwidth Rate Allocation	DOCSIS 1.1 for the Cisco CMTS Routers
Dynamic Bandwidth Sharing	Dynamic Bandwidth Sharing on the Cisco CMTS Router

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DOCSIS WFQ Scheduler

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

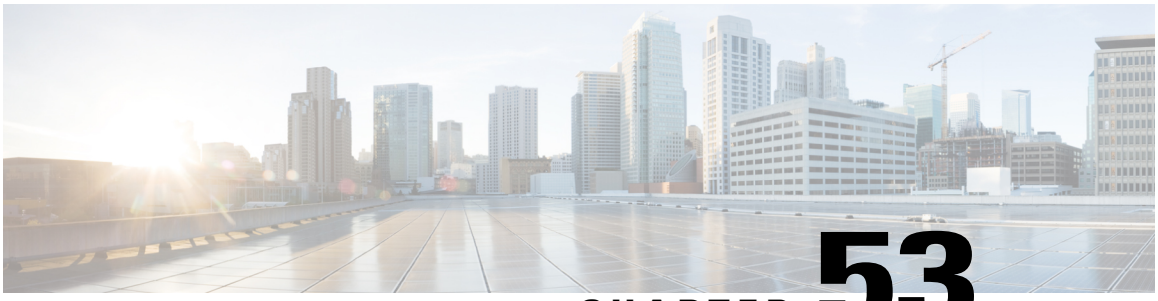
Table below lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(33)SCB or a later releases release appear in the table.

Table 148: Feature Information for DOCSIS WFQ Scheduler

Feature Name	Releases	Feature Information
DOCSIS WFQ Scheduler	12.2(33)SCB	The DOCSIS WFQ Scheduler provides output scheduling services on DOCSIS downstream interfaces. Cisco IOS Release 12.2(33)SCB introduces this feature on the Cisco uBR10012 Universal Broadband Router.

Feature Name	Releases	Feature Information
DOCSIS WFQ Scheduler	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduces the option to configure user-defined priorities to map DOCSIS priority value to an excess ratio value. Using this feature, you can configure priorities in the downstream direction rather than using the default rates. The following command was introduced: cable downstream qos wfq weights
Enhanced Rate Bandwidth Allocation	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. Dual token bucket based shaper is used to support ERBA on the uBR-MC88V line card for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following section provides information about this feature:
DOCSIS 3.0 Downstream Bonding Support with Bonding Group Dynamic Bandwidth Sharing	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following commands were introduced or modified: • **show cable modem** • **show interface cable service-flow** • **show interface integrated-cable** • **show interface wideband-cable queue**
Suppressing Downstream and Upstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems	12.2(33)SCB10	Support was added to restrict sending of the DOCSIS 3.0 TLVs to DOCSIS 1.X and DOCSIS 2.0 cable modems. A new command cable service attribute withhold-TLVs was introduced.

Feature Name	Releases	Feature Information
Optimization of queue size	12.2(33)SCG	Default queue size for the DOCSIS service flows (with bandwidth greater than 150 Mbps) is increased. A new command **cable queue-limit** was introduced



CHAPTER 53

Dynamic Bandwidth Sharing on the Cisco CMTS Router

First Published: February 25, 2008

Last Updated: November 29, 2010

The Cable Modem Termination System (CMTS) enables dynamic bandwidth sharing (DBS) on modular cable (MC), integrated cable (IC), and wideband (WB) cable interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Dynamic Bandwidth Sharing

Table below shows the hardware compatibility prerequisites for the Dynamic Bandwidth Sharing on the Cisco CMTS Router feature.

Table 149: Cable Hardware Compatibility Matrix for Dynamic Bandwidth Sharing

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(23)BC1 and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[100]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V
Cisco uBR7246VXR Universal Broadband Routers	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

100 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

Restrictions for Dynamic Bandwidth Sharing

- The bandwidth sharing state of a modular, integrated, or wideband cable interface can be changed only when the interface is administratively shutdown.

Information About Dynamic Bandwidth Sharing

The following sections provide information on DBS:

DBS for Modular, Integrated, and Wideband Cable Interfaces

Prior to DOCSIS 3.0 standards, cable service flows were associated with a single cable interface, which in turn corresponded to a physical downstream on a line card. Under DOCSIS 3.0 standards, cable service flows can be associated with more than one downstream channel.

DBS is the dynamic allocation of bandwidth for MC, IC, and WB cable interfaces sharing the same downstream channel. The bandwidth available to each MC, IC, WB cable, or narrowband channel is not a fixed value—it depends on the configuration and the traffic load on the MC, IC, or WB cable.

The available bandwidth for data traffic is calculated using the following formula: Actual Line Rate – (Bandwidth used by MAC Management Messages [MMM] + Bandwidth loss due to DOCSIS header)

The bandwidth required by MMM depends on the CMTS configuration. The maximum bandwidth reserved for MMM is 4 percent (if the MMM uses less than 4 percent of bandwidth, the remaining unused bandwidth is available for the data traffic).

DBS enables high burst rates with DOCSIS 2.0 cable modems as well as DOCSIS 3.0 cable modems. The DBS feature continues working across line card and performance routing engine (PRE) switchovers with no loss of functionality.

DBS Configuration

Dynamic bandwidth sharing and static bandwidth allocations are configured at the MC, IC, or WB cable interface level. By default, bandwidth for an MC, IC, or WB cable channel is statically allocated. When DBS is enabled on an interface, the static bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding interface. The interface CIR value represents the guaranteed portion of the interface bandwidth and is used for admission control of the service flows with minimum reserved rate. When DBS is enabled, you can also specify the remaining ratio value of the excess bandwidth for the interface. If DBS is enabled and no bandwidth percentage is specified, no bandwidth is reserved for the MC, IC, or WB cable interface and the interface is effectively in protocol down state.

Dynamic bandwidth sharing does not preclude static bandwidth configuration. If a static portion of bandwidth is configured on any RF channel that one or more DBS-enabled channel utilizes, that portion is subtracted from the CIR value of the RF link. Therefore, such a portion is always reserved and is not available to dynamic MC, IC, or WB cable interfaces.

Note Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB/MC/IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.

How to Configure Dynamic Bandwidth Sharing

This section contains the following procedures:

Configuring DBS for a Modular Cable Interface

To configure DBS for an MC interface on the Cisco uBR10012 router, use the **cable dynamic-bw-sharing** command in interface configuration mode.

Note The interface must be administratively shutdown before DBS can be configured on the MC interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface modular-cable** *slot* /*subslot* /*port* :*nb-channel-number* **Example:** `Router(config)# interface modular-cable 1/0/0:1`	Configures a modular cable interface. • *slot* —Chassis slot number of the cable interface line card. Cisco uBR10012 router: The valid range for line card is from 5 to 8 and slots 1 and 3 can be used for SIPs. • *subslot* —(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port* —Downstream port number. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *nb-channel-number*—Narrowband channel number.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	[**no**] **cable dynamic-bw-sharing** **Example:** `Router(config-if)# cable dynamic-bw-sharing`	Enables dynamic bandwidth sharing (DBS) on the modular cable interface. Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface. **Note** Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which dynamic bandwidth sharing is configured.
Step 7	**cable rf-bandwidth-percent***percent-value* [**remaining ratio** *excess-value*] **Example:** `Router(config-if)# cable rf-bandwidth-percent 45 remaining ratio 22`	Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default *percent-value* is 0. The *percent-value* range is 1–96. • If dynamic bandwidth sharing is enabled, the **remaining ratio** option is available. The bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding interface. • The *excess value* - argument specifies the ratio of the excess bandwidth that can be allocated to the modular cable channel. The default *excess value* - is 1. The *excess value* - range is 1–100.

Configuring DBS for a Wideband Cable Interface

To configure DBS for a wideband cable interface, use the **cable dynamic-bw-sharing** command in interface configuration mode for WB cable.

Note The interface must be administratively shutdown before DBS can be configured on the wideband cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*port* }:*wideband-channel*	Configures a wideband cable interface. • *slot* —Chassis slot number of the cable interface line card.

	Command or Action	Purpose
	Example: `Router(config)# interface wideband-cable 1/0/0:0`	Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot* —(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port* —Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *wideband-channel*—Wideband channel number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid values are from 0 to 5. Cisco uBR10012 router: The valid range is from 0 to 11.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	**cable dynamic-bw-sharing** **Example:** `Router(config-if)# cable dynamic-bw-sharing`	Enables dynamic bandwidth sharing (DBS) on the wideband cable interface. Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface. **Note** Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the **no cable dynamic-bw-sharing** command.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which dynamic bandwidth sharing is configured.
Step 7	**cable rf-channel***rf-port* [**bandwidth-percent** *bw-percent*] [**remaining ratio***excess-value*] **Example:** `Router(config-if)# cable rf-channel 10 bandwidth-percent 50 remaining-ratio 5`	Associates an RF channel on a Wideband SPA with a wideband channel and allocates bandwidth. The range for **bandwidth-percent** is 1–100. If **bandwidth-percent** is not used, the default bandwidth value is 100 percent. The **remaining-ratio** option is only available if DBS is enabled. The default *excess-value* is 1. The range for *excess-value* is 1–100.

Configuring DBS for an Integrated Cable Interface

To configure DBS for an integrated cable interface, use the **cable dynamic-bw-sharing** command in interface configuration mode.

Note The interface must be administratively shutdown before DBS can be configured on the integrated cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface integrated-cable** {*slot*/*port* | *slot*/*subslot*/*port* }:*rf-channel* **Example:** `Router(config)# interface integrated-cable 1/0/0:0`	Enters the cable interface mode. • *slot* —Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *rf-channel*—RF channel number with a range of 0 to 3.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	**cable dynamic-bw-sharing**	Enables dynamic bandwidth sharing on the wideband cable interface.

	Command or Action	Purpose
	Example: `Router(config-if)# cable dynamic-bw-sharing`	Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface. **Note** Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface where dynamic bandwidth sharing is configured.
Step 7	**cable rf-channel** *rf-port* [**bandwidth-percent** *bw-percent*] [**remaining ratio** *excess-value*] **Example:** `Router(config-if)# cable rf-channel 10 bandwidth-percent 50 remaining-ratio 5`	Enables either static or dynamic bandwidth percentage sharing for an IC interface in interface configuration mode. • *bw-percent*—Static bandwidth allocation of a downstream RF channel. The range is 1 to 100%. The default is 0. • **remaining ratio**—(Optional) Indicates the ratio of the remaining or excess bandwidth that can be allocated to the modular cable channel. This option is available only when dynamic bandwidth sharing is enabled. Run the **cable dynamic-bw-sharing** command to enable DBS. • *excess-value*—Value of excess bandwidth that can be allocated to the cable channel. The range is from 1 to 100. The default value is 1.

Verifying Configuration of DBS

To verify the configuration of the CMTS DBS, use the **show** commands described below.

Cisco uBR10012 Universal Broadband Router

To view the parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command for either modular cable or wideband cable interfaces.

Modular cable interface

```
Router(config)# interface modular-cable 1/0/0:1
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue modular-cable 1/0/0:1
Link Queues :
QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  420   19661/19661        1/1        65535/65535      0       Inactive
```

Wideband cable interface

```
Router(config)# interface wideband-cable 1/0/0:0
...
```

```
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue wideband-cable 1/0/0:0
Link Queues :
QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  419   32768/32768        1/1        65535/65535      0       Inactive
  566   19661/19661        1/1        65535/65535      1       Inactive
```

Cisco uBR7200 Series Universal Broadband Router

To view the DBS configuration on the Cisco uBR7200 series universal broadband router, use show interface wideband-cable slot/port:wideband-channel dbs and show interface integrated-cable slot/port:rf-channel dbs commands as shown below:

Wideband cable interface

```
Router(config)# interface wideband-cable 5/1:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show
interface wideband-cable 5/1:0 dbs
        Dynamic Bandwidth Sharing is enabled
        bg_rf_channel_bitmap_local 70, active 0
        RF 4: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
        RF 5: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
        RF 6: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
                dbs state: start:4, end:6
```

Integrated cable interface

```
Router(config)# interface integrated-cable 5/1:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show
interface integrated 5/1:0 dbs
        Dynamic Bandwidth Sharing is enabled
        active 0
        RF 4: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
              deficit counter 0, quantum 0
              ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
              dbs_pct: 100, remain_bytes: 0, if range: 7-7
```

Enabling DBS Debug

To enable specific DBS debug output, use the **debug cr10k-rp dbs-queue** command on the Cisco uBR10012 router and the debug cable dbs command on the Cisco uBR7200 series routers as shown in the following examples:

```
Router# debug cr10k-rp dbs-queue
CR10K RP debug dynamic BG link queue setup debugging is on
Router# debug cable dbs
DBS for cable 8x8 LC debugging is on
```

Note Routine use of the **debug cr10k-rp dbs-queue** and debug cable dbs commands is not recommended.

Configuration Examples for Dynamic Bandwidth Sharing

This section provides the following configuration examples:

Example: Configuring DBS on a Modular Cable Interface

In the following example, DBS is enabled on modular cable interface 1. Because DBS is enabled, the percent value is converted to a committed information rate (CIR) of 45, which means the modular cable channel is guaranteed 45 percent of the bandwidth. The ratio of excess bandwidth is assigned a value of 22, which means that if there is excess bandwidth available, a remaining ratio of 22 can be assigned to the MC channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface modular-cable 1/0/0:1
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-bandwidth-percent 45 remaining ratio 22
```

Example: Configuring DBS on a Wideband Cable Interface

In the following example, DBS is enabled on wideband channel 0. Because DBS is enabled, the percent value is converted to a CIR value of 50, which means the wideband cable channel is guaranteed 50 percent of the bandwidth. The *excess-value* is assigned a value of 5, which means that if there is excess bandwidth available, a remaining ratio of 5 can be assigned to the wideband channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface wideband-cable 1/0/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Cisco uBR7200 Series Universal Broadband Routers

```
configure terminal
interface wideband-cable 1/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Example: Configuring DBS on an Integrated Cable Interface

In the following example, DBS is enabled on integrated channel 0. Because DBS is enabled, the percent value is converted to a CIR value of 50, which means the integrated cable channel is guaranteed 50 percent of the bandwidth. The *excess-value* is assigned a value of 5, which means that if there is excess bandwidth available, a remaining ratio of 5 can be assigned to the integrated channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface integrated-cable 1/0/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Cisco uBR7200 Series Universal Broadband Routers

```
configure terminal
interface integrated-cable 1/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
```
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cisco uBR10012 universal broadband router or Cisco uBR7200 series universal broadband router and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at:

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

Additional References

The following sections provide references related to the dynamic bandwidth sharing (DBS) on the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco IOS CMTS cable commands	See the *Cisco IOS CMTS Cable Command Reference* at: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Dynamic Bandwidth Sharing

Table below lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation

.

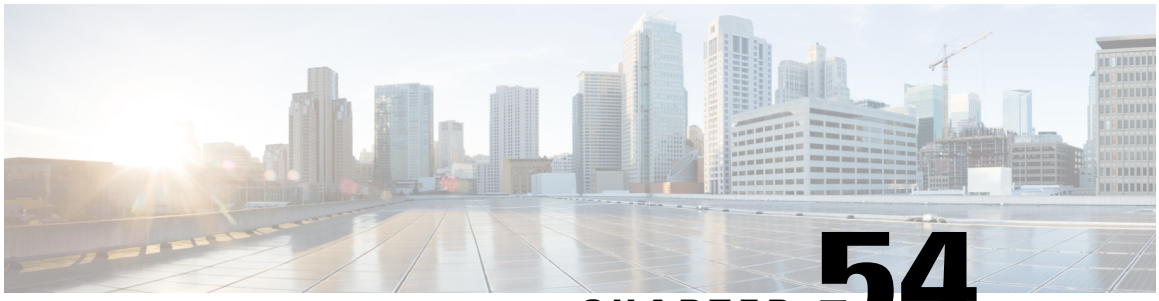
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 150: Feature Information for Dynamic Bandwidth Sharing

Feature Name	Releases	Feature Information
CMTS Dynamic Bandwidth Sharing	12.3(23)BC1	The Cisco CMTS new feature enables dynamic bandwidth sharing on a modular cable or wideband cable interface. The following commands were introduced or modified by this feature: • **cable dynamic-bw-sharing** • **cable rf-bandwidth-percent** • **cable rf-channel** • **debug cr10k-rp dbs-queue** • **show pxf cable controller** • **show pxf cpu queue**

Feature Name	Releases	Feature Information
CMTS Dynamic Bandwidth Sharing	12.2(33)SCD	Support on the Cisco uBR7225VXR and Cisco uBR7246VXR routers was added. The following commands were introduced or modified: • **debug cable dbs** • **interface integrated-cable** • **interface wideband-cable** • **show interface integrated-cable** • **show interface wideband-cable**



CHAPTER 54

Fairness Across DOCSIS Interfaces

First Published: June 20, 2011

The Fairness Across DOCSIS Interfaces feature introduces an adaptive mechanism to effectively distribute reservable bandwidth for committed information rate (CIR) flows and fair bandwidth for best-effort (BE) service flows across adjacent bonding groups (BGs).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Fairness Across DOCSIS Interfaces

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 151: Fairness Across DOCSIS Interfaces for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC5X20H[101] • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[102]	Cisco IOS Release 12.2(33)SCF and later releases • Cisco Wideband SIP and Cisco Wideband SPA • Cisco 10000 Series SIP-600 and Cisco Wideband SPA Cisco IOS Release 12.2(33)SCH and later releases • Cisco Next Generation Wideband SPA

101 When Fairness Across DOCSIS Interfaces feature is enabled, the Cisco uBR-5X20H cable interface line card can only act as a Guardian or MAC domain host as bonding is not supported on the card.

102 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

Note The term 'Bonding Group (BG)' is used in this document to refer to all the integrated-cable (IC), modular-cable (MC), and wideband-cable (WC) interfaces in the context of Fairness Across DOCSIS Interfaces feature context. The IC and MC interfaces are considered as a single-channel BG.

Restrictions for Fairness Across DOCSIS Interfaces

- The CIR flows cannot reserve all the RF bandwidth. The CIR flows can only reserve 90 percent[103] of the RF bandwidth that is not statically reserved by the "bandwidth-percent", in addition to the legacy CIR bandwidth.
- It is recommended that the CIR reservation be cleared before disabling Fairness Across DOCSIS Interfaces feature to ensure that the CIR reservation is not more than the static reservable bandwidth specified by

103 The reservable bandwidth for CIR flows consists of static and dynamic portions. By default, the static portion of bandwidth is assigned from the legacy configuration. The dynamic portion of bandwidth comes from the headroom left on each RF channel for BE traffic.

the “bandwidth-percent” in legacy configuration. This is to prevent CIR over-subscription after disabling Fairness Across DOCSIS Interfaces feature.

- The effect of Fairness Across DOCSIS Interfaces feature depends on topology and flow distribution. In certain cases, Fairness Across DOCSIS Interfaces feature may not achieve BE fairness or maximum CIR utilization.
- Fairness Across DOCSIS Interfaces feature applies only to dynamic bandwidth sharing (DBS) enabled IC and WB interfaces.

Information About Fairness Across DOCSIS Interfaces

The Fairness Across DOCSIS Interfaces feature is an enhancement over the DOCSIS WFQ scheduler. It enables downstream CIR service flows to be admitted on the interfaces over the thresholds defined in the legacy configuration (that is, “bandwidth-percent” or “max-reserved-bandwidth”). For example, the feature enables large CIR flows (like multicast service flows) to be admitted when the current parameters cannot guarantee enough bandwidth. However, its success rate depends on the allocation and reservation of the bandwidth for cable interfaces within common RF channels.

This feature also ensures fair bandwidth for downstream BE service flows across cable interfaces with common RF channels. The per-flow bandwidth of all active service flows on the adjacent BGs are balanced periodically in proportion to their DOCSIS traffic priority (traffic priority + 1) for downstream BE service flows. This bandwidth, available for BE traffic, can also be used to admit additional CIR flows.

Note For information about DOCSIS traffic priority, see DOCSIS WFQ Scheduler on the Cisco CMTS Routers guide.

How to Configure Fairness Across DOCSIS Interfaces

This section describes the following tasks that are required to implement Fairness Across DOCSIS Interfaces feature:

Configuring Fairness Across DOCSIS Interfaces

This section describes how to enable Fairness Across DOCSIS Interfaces feature on the cable interfaces. The configuration is applied to all WB, MC or IC interfaces on the router.

Restriction We recommend that you clear the CIR reservation before disabling the Fairness Across DOCSIS Interfaces feature to ensure that CIR reservation is not more than the static reservable bandwidth specified by the “bandwidth-percent” in the legacy configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable acfe enable** **Example:** `Router(config)# cable acfe enable`	Enables Fairness Across DOCSIS Interfaces feature on the cable interfaces.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Maximum Excess Information Rate Ratio

This section describes how to configure the maximum Excess Information Rate (EIR) ratio between the BE bandwidth among adjacent BGs.

The EIR ratio is used to maintain the maximum EIR bandwidth difference between BGs. It helps to prevent BGs (which has only a few active BE service flows) from getting very low or zero EIR bandwidth. Otherwise, these BGs will not be able to admit CIR flows as they get only very low EIR bandwidth.

For example, there are two BGs sharing the same RF channel, with BG1 having 1000 active BE service flows and BG2 having none. If “max-eir-ratio” is not used, BG1 gets all the bandwidth leaving no bandwidth for BG2. When a voice CIR tries for bandwidth at BG2, it will get rejected. If “max-eir-ratio” is set at 10, BG2 gets about 10 percent of the QAM that is sufficient to admit the voice CIR. The ‘max-eir-ratio’ is a trade-off between perfect fairness and CIR utilization. It means, compromising 'flow fairness' to prevent some BGs from getting all the bandwidth leaving the other BGs with none.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable acfe max-eir-ratio** *eir-ratio* **Example:** `Router(config)# cable acfe max-eir-ratio 20`	Configures the maximum EIR ratio between the BE bandwidth among adjacent BGs.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Constant Excess Information Rate Demand

This section describes how to configure the constant excess information rate (EIR) demand for a bonding group (BG). EIR demand is a unitless value that is used to determine relative bandwidth ratio between BGs.

An active EIR flow with DOCSIS priority-0 is given 1000 units of demand in ACFE module. Therefore a BG with constant-eir-demand set to 1 will get no more than 1/1000 of the bandwidth of a single service flow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable acfe constant-eir-demand** *value*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable acfe constant-eir-demand** *value* **Example:** `Router(config)# cable acfe constant-eir-demand 20`	Configures the constant EIR demand as 20 for a BG.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Maximum Bonus Bandwidth

This section describes how to configure the maximum usable bonus bandwidth for a BG.

Bonus bandwidth is the additional bandwidth provided by the Fairness Across DOCSIS Interfaces feature to each BG for CIR reservation. In the default maximum bonus bandwidth configuration, a single BG can reserve all the underlying RF bandwidth. When the maximum bonus is set, the AC module will not admit CIR flows above that setting even if the scheduler has guaranteed more bandwidth. This will effectively prevent BGs from being starved for CIR flows.

Note The **cable acfe max-bonus-bandwidth** command configuration is applicable only for the new incoming CIR flows. It will not terminate the existing CIR flows that exceeds the **max-bonus-bandwidth** .

Restriction If the maximum bonus bandwidth is less than the current CIR reservation on an interface, no new CIR flows are admitted until the CIR reservation drops below the maximum bonus bandwidth configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**wideband-cable** | **modular-cable** | **interface-cable** }*slot*/*subslot* /*port* :*interface-num* **Example:** `Router(config)# interface wideband-cable 1/0/0:0`	Specifies the interface to be configured. **Note** The valid values for the arguments depend on CMTS router and cable interface line card. See the hardware documentation for your router chassis and cable interface line card for supported values.
Step 4	**cable acfe max-bonus-bandwidth** *bonus-bandwidth* **Example:** `Router(config-if)# cable acfe max-bonus-bandwidth 1000000`	Configures the maximum usable bonus bandwidth for a BG.
Step 5	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Fairness Across DOCSIS Interfaces

To monitor the Fairness Across DOCSIS Interfaces feature, use the following procedures:

Verifying Reservable Bandwidth

To display the reserved and reservable bandwidth for a particular interface, use the **show interface {wideband-cable | modular-cable | integrated-cable}** command as shown in the example:

```
Router# show interfaces wideband-cable 1/0/0:1 downstream
Total downstream bandwidth 3235 Kbps
Total downstream reserved/reservable bandwidth 0/200 Kbps
Total downstream guaranteed/non-guaranteed bonus bandwidth 66618/9972 Kbps
!
```

The “reservable bandwidth” is a part of the guaranteed bandwidth from the legacy configuration. When the Fairness Across DOCSIS Interfaces feature is disabled, values of both the “guaranteed bonus bandwidth” and “non-guaranteed bonus bandwidth” are zero. When the feature is enabled, the “reservable bandwidth” and “guaranteed bonus bandwidth” represents the maximum CIR that can be reserved on the interface. Unicast CIR flows exceeding this limit are rejected. The additional “non-guaranteed bonus bandwidth” allows the multicast CIR flows to pass the AC module. However, the service flow may not be created successful because the bandwidth comes from the shared pool.

Note The “guaranteed bonus bandwidth” and “non-guaranteed bonus bandwidth” are part of the bandwidth provided by the maximum bonus bandwidth configuration. The “non-guaranteed bonus bandwidth” is expected to be used only by multicast service flows in Cisco IOS Release 12.2(33)SCF.

To display the reserved and reservable bandwidth for a particular interface, use the **show cable admission-control interface** command as shown in the example:

```
Router# show cable admission-control interface wideband-cable 1/0/0:1 verbose
Interface Wideband-Cable1/0/0:1
Configured AC Max Reservable Bandwidth = 6000000 bps
 Resource - Downstream Bandwidth
 -------------------------------
Bkt    Name   Minor # of  Major # of  Excls # of  Non-Ex Curr. Curr. Conf  # of
No            Level Times Level Times Level Times Level  Resv  Ovrsb Level Rej
1             0     0     0     0     0     0     0  *    0.0   0.0  G       0
2             0     0     0     0     0     0     0  *    0.0   0.0  G       0
3             0     0     0     0     0     0     0  *    0.0   0.0  G       0
4             0     0     0     0     0     0     0  *    0.0   0.0  G       0
5             0     0     0     0     0     0     0  *    0.0   0.0  G       0
6             0     0     0     0     0     0     0  *    0.0   0.0  G       0
7             0     0     0     0     0     0     0  *    0.0   0.0  G       0
8             0     0     0     0     0     0     100*   50.0   0.0  G       0
 Note: * indicates that the thresholds are implicit
WB-NB CIR for Wideband-Cable1/0/0:1
CIR Values for Cable8/1/4
Bkt SFAC BW    Rsvd CIR   Reject #
0   0          0          0
1   0          0          0
2   0          0          0
3   0          0          0
4   0          0          0
5   0          0          0
6   0          0          0
7   4500000    3000000    0
Available Guaranteed Bonus BW (bps): 30375000
Available Non-guaranteed Bonus BW (bps): 0
WB Multicast CIR Utilization
Bkt SFAC BW    Rsvd CIR   Reject #
0   0          0          0
1   0          0          0
2   0          0          0
3   0          0          0
4   0          0          0
5   0          0          0
6   0          0          0
7   1500000    0          0
Available Guaranteed Bonus BW (bps): 30375000
Available Non-guaranteed Bonus BW (bps): 0
```

Verifying Global Fairness Across DOCSIS Interfaces Status and Statistics

To display the global status and statistics of the Fairness Across DOCSIS Interfaces feature, use the **show cable acfe summary** command as shown in the example:

```
Router# show cable acfe summary
ACFE state: Enabled
EIR Rebalance period (secs): 5
EIR Rebalance invocations:   254
CIR Acquire rate/limit:      100/100
CIR Acquire invocations:     0
CIR Acquire throttled:       0
CIR Oversubscriptions:       0
```

```
Maximal EIR ratio:           10
Constant EIR demand:         2
```

Verifying Per-Controller Fairness Across DOCSIS Interfaces Status and Statistics

To display the status and statistics for each controller interface, use the **show cable acfe controller** command as shown in the following example:

```
Router# show cable acfe controller modular-cable 1/0/0
EIR Rebalance invoked: 301832
Adaptive CIR granted:  0
Adaptive CIR rejected: 0
Total clusters: 2
!
```

The BG clusters span across multiple channels and are used as a means to share the underlying RF channel bandwidth dynamically.

```
RF      FlexBW
0       30375
1       30375
RF      FlexBW
2       30375
3       30375
```

Verifying Per-Interface Fairness Across DOCSIS Interfaces Status and Statistics

To display the status and statistics for each interface, use the **show cable acfe interface** command as shown in the following example:

```
Router# show cable acfe interface wideband-cable 1/0/0:1
EIR Demand (raw/scale):   0/1
Per-Flow EIR BW (kbps):   19125
Guar Bonus BW (kbps):     19125
Non-guar Bonus BW (kbps): 38250
Reserved Bonus BW (kbps): 0
!
```

The EIR demand is the number of active BE service flows for each BG within a specific time period weighted by DOCSIS priority. The EIR portion is adjusted periodically in proportion to the EIR demand for each BG within the same BG cluster.

```
AC Max Reserved Bandwidth: 200 kbps
Bucket Reservations (kbps):
!
```

For information on Bucket Reservations, see the Service Flow Admission Control for the Cisco CMTS Routers guide.

Troubleshooting

The following **debug** commands help you troubleshoot an improper configuration:

- **debug cable acfe —**Enables debug operation for the Fairness Across DOCSIS Interfaces feature. You should run the debug cable acfe command first to enable other debug options listed below.
- **debug cable acfe algorithm —**Provides debugging information on internal operations of algorithms.
- **debug cable acfe all —**Provides debugging information of all cable events.

- **debug cable acfe filter** —Provides debugging information after applying the filter to limit the debug output.
- **debug cable acfe filter controller** —Provides debugging information on specific controllers.
- **debug cable acfe cluster** —Provides debugging information on specific clusters.
- **debug cable acfe hccp** —Provides debugging information on high availability and Hot Standby Connection-to-Connection Protocol (HCCP) activities.
- **debug cable acfe process** —Provides debugging information on process activities.
- **debug cable acfe read**—Provides debugging information from the system.
- **debug cable acfe topology** —Provides debugging information on cluster topology.
- **debug cable acfe verbose** —Provides debugging information on all internal data.
- **debug cable acfe write** —Provides debugging output to the router.

For detailed information on these and other debug commands, see the Cisco IOS CMTS Cable Command Reference guide.

Configuration Examples for Fairness Across DOCSIS Interfaces

This section lists the following sample configurations for the Fairness Across DOCSIS Interfaces feature on a Cisco CMTS router:

Example: Fairness Across DOCSIS Interfaces

The following sample configuration shows Fairness Across DOCSIS Interfaces feature enabled on the router:

```
Current configuration : 39682 bytes
!
! Last configuration change at 04:30:02 UTC Wed Jan 19 2
! NVRAM config last updated at 04:23:17 UTC Wed Jan 19 2
!
version 12.2
!
cable clock dti
cable acfe enable
!
.
.
.
```

Example: Maximum EIR Demand Ratio

The following sample configuration shows maximum EIR demand ratio configured on the router:

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
!
```

The effect of the **cable acfe max-eir-ratio** command is demonstrated using a simple BG cluster, a 37.5 Mbps RF bandwidth shared by an MC and WB interface. The interfaces are configured as given in the following configuration example:

```
!
interface Modular-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
!
interface Wideband-Cable1/0/0:0
cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
end
!
```

On this RF channel, 20 percent of the bandwidth is reserved by the 'bandwidth-percent' allowing Fairness Across DOCSIS Interfaces feature to use 27 Mbps, that is: (100 - 20) * 90 * 37.5). If the 'max-eir-ratio' is above 100 and the WB interface has 99 active BE flows and the MC interface has only 1 BE flow, then MC interface gets only 270 kbps, that is 1/(1+99)*27 of the bonus bandwidth. The BE traffic enjoys perfect fairness here. However, it is not possible to admit a unicast CIR flow beyond 270 kbps on the MC interface, as it would exceed the bonus bandwidth. If the 'max-eir-ratio' is set to 10, then the MC interface is treated to have 99/10 flows on it, resulting in a higher bonus bandwidth allocation. The 'max-eir-ratio' is a trade-off between perfect fairness and CIR utilization.

Example: Constant EIR Demand

The following sample configuration shows constant EIR demand on the router:

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
cable acfe constant-eir-demand 2
!

!
interface Modular-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
 cable acfe constant-eir-demand 2

!
interface Wideband-Cable1/0/0:0
cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
 cable acfe constant-eir-demand 2

end
!
```

Example: Maximum Bonus Bandwidth

The following sample configuration shows the maximum bonus bandwidth enabled on the router:

```
Building configuration...
Current configuration : 274 bytes
!
interface Wideband-Cable1/0/0:0
```

```
cable bundle 1
cable rf-channel 0 bandwidth-percent 10
cable acfe max-bonus-bandwidth 10000
end
!
```

In this per-interface configuration, even if the Fairness Across DOCSIS Interfaces feature guarantees more than 10 Mbps for a WB interface, the AC module will not pass more than 10 Mbps bandwidth above the legacy reservable bandwidth.

```
!
.
.
.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS CMTS Cable Command Reference	Cisco IOS CMTS Command Reference
Dynamic Bandwidth Sharing	Dynamic Bandwidth Sharing on the Cisco CMTS Router
DOCSIS WFQ Scheduler	DOCSIS WFQ Scheduler on the Cisco CMTS Routers
Service Flow Admission Control for the Cisco CMTS Routers	Service Flow Admission Control for the Cisco CMTS Routers

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Fairness Across DOCSIS Interfaces

Table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 152: Feature Information for Fairness Across DOCSIS Interfaces

Feature Name	Releases	Feature Information
Fairness Across DOCSIS Interfaces	12.2(33)SCF	The Fairness Across DOCSIS Interfaces feature introduces an adaptive mechanism to effectively distribute reservable bandwidth for CIR flows and fair bandwidth for BE service flows across adjacent BGs. The following commands were introduced or modified: • **cable acfe enable** • **cable acfe max-eir-ratio** • **cable acfe max-bonus-bandwidth** • **debug cable acfe** • **debug cable acfe filter** • **show cable acfe controller** • **show cable acfe interface** • **show cable acfe summary** • **show cable admission-control** • **show cr10k-rp controller** • **show interface integrated-cable** • **show interface modular-cable** • **show interface wideband-cable**

CHAPTER 55

Modular Quality of Service Command-Line Interface QoS on the Cisco CMTS Routers

First Published: December 18, 2008 Last Updated: July 11, 2012

The Modular Quality of Service Command-Line Interface (MQC) is designed to simplify the configuration of Quality of Service (QoS) on the Cisco CMTS routers by defining a common command syntax and resulting set of QoS behaviors across platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for MQC QoS

Table below shows the Cisco cable modem termination system (CMTS) hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 153: MQC QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases releases** • PRE2 **Cisco IOS Release 12.2(33)SCB and later releases releases** • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases releases** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later releases releases** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later releases releases** • Cisco uBR-MC3GX60V [104]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later releases** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V [105]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later releases** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V

104 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.
105 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Note The combination of PRE4 and Cisco Half-Height Gigabit Ethernet (HHGE) is not supported in the same chassis.

Restrictions for MQC QoS

- The sum of all priority traffic running on a given port must be less than or equal to 90 percent of the port bandwidth.
- The 802.1p and Multiprotocol Label Switching (MPLS) Matching and Marking feature is currently supported only on Cisco uBR10012 routers.
- The MPLS Pseudowire for Cable L2VPN (Any Transport Over MPLS [AToM]) feature does not support matching and marking based on IP header fields. AToM supports only the matching and marking of experimental (EXP) bits.
- The Transport Layer Security (TLS) and cable dot1q L2VPN do not support the Input service policy and IPv6 service policy.
- PRE2 does not support IPv6 class of service (CoS) policy.
- MQC must be configured on the logical interface of a tunnel for the Cisco uBR10012 router.

Information About MQC QoS

Quality of Service (QoS) is supported on WAN interfaces using the standard MQC. The MQC CLI structure allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and QoS features. A traffic class is used to select traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

Classifying Traffic

The Cisco uBR10012 Universal Broadband Router must differentiate traffic before it can apply appropriate QoS actions to the traffic. You can use an MQC CLI element called a *class map* to define traffic classification rules or criteria.

Class maps organize data packets into specific categories called classes that can receive user-defined QoS policies. The traffic class defines the classification rules for packets received on an interface.

Configuring QoS Policy Actions and Rules

After classifying the traffic, the Cisco uBR10012 Universal Broadband Router must be configured to handle the traffic that meets the matching criteria. The MQC CLI element *policy map* is used to create QoS policies and configure QoS actions and rules to apply to packets that match a particular traffic class.

A policy map associates a traffic class with one or more QoS actions. While configuring a policy map, you can specify a class map name and configure the actions you want the router to take on the matching traffic. However, before creating class policies in a policy map, the class classification criteria must be configured in a class map.

Whenever you modify a class policy of a policy map, class-based weighted fair queuing (CBWFQ) is notified and new classes are installed as part of the policy map in the CBWFQ system.

Attaching Service Policies to an Interface

After creating and configuring a traffic policy, you should attach the policy to an interface. A policy can be applied to packets in either direction, inbound or outbound. An interface can have different service policies for incoming and outgoing packets.

802.1p CoS

The 802.1p CoS feature introduces QoS-based matching and marking to VLAN user priority bits to provide QoS service on the Gigabit Ethernet WAN interface for 802.1q packets.

The 802.1p CoS marking is a QoS action like the “set ip precedence” that sets the user priority bits for traffic prioritization. CoS refers to the three bits in the VLAN header that is used to indicate the IEEE 802.1p priority of the Ethernet frame as it passes through a switched network.

Marking is a way to identify packet flows to differentiate them. Packet marking enables partitioning of the network into multiple priority levels, or classes of service. During network congestion, the priority marked packets are offered a higher priority than normal packets.

The 802.1p input packets are classified at eight different QoS levels (0 to 7) based on the VLAN user priority bits. The packet classification is specified through the MQC using ‘match’ statements within the class-map command.

On the Cisco CMTS router, 802.1p CoS matching is provided only for the input VLAN tagged frames. The user priority bits matching is not available for TLS and dot1q L2VPN packets.

For 802.1q output packets, QoS marking is done at the VLAN header to modify VLAN user priority bits. QoS services use these priority bit settings to gain traffic priority during times of congestion. For upstream TLS and dot1q L2VPN packets, user priority bits marking is done on the WAN interface.

Note For information on QoS, see Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide .

MPLS Short-Pipe

The MPLS Short-Pipe Mode feature introduces QoS-based matching and marking of MPLS EXP bits to provide QoS service on the WAN interface for MPLS packets. The three bit EXP define QoS treatment for a packet. The EXP bits support up to eight classes of traffic.

When an IP packet is sent from one site to another, the IP precedence field specifies QoS. Based on the IP precedence marking, the packet is given the treatment configured for that QoS. In an MPLS network, IP precedence value is copied to the MPLS EXP field during label imposition by default.

MPLS marking is a QoS action like the “set ip precedence”. Marking sets different values for the MPLS EXP field. This enables service providers to set the priority for packets transported through their networks. The packet classification criteria is specified through the MQC using ‘match’ statements within the class-map command.

MPLS CoS matching provides the QoS classification function based on the EXP bits of the label entry. For MPLS input packets, QoS classification is done to provide different levels of QoS based on the MPLS EXP bits. For MPLS output packets, the QoS marking is done at the MPLS label header to modify EXP bits.

Note IP ToS will be inactive when the MPLS EXP classification is active as both MPLS EXP and IP ToS shares the same field.

MPLS CoS treats AToM packets as general MPLS packets. For upstream AToM packets, marking is done for EXP bits on the imposition label. For downstream AToM packets, classification is done based on the EXP bits.

MPLS Tunneling

Tunneling is the ability of QoS to be transparent from one edge to the other edge of the network. A tunnel starts on label imposition, and ends at label disposition. When the label is stripped off, the packet goes out as an MPLS packet with a different Per-Hop Behavior (PHB) layer underneath or as an IP packet with and IP PHB layer.

MPLS QoS supports the following tunneling modes:

Uniform Mode

In this mode, packets are treated uniformly across the network. All the customers of the MPLS network use the same IP precedence settings. The IP precedence value and the MPLS EXP bits always correspond to the same PHB.

Short Pipe Mode

This mode provides a distinct MPLS PHB layer (on top of the IP PHB layer) across the entire MPLS network, allowing customers of a service provider to implement their own IP PHB marking scheme on the MPLS network.

For more information on tunneling, see DiffServ Tunneling Modes for MPLS Networks at http://www.cisco.com/en/US/tech/tk436/tk428/tech_tech_notes_list.html .

Input MQC Support on the Cable Bundle Interfaces

The Input MQC Support on the Cable Bundle Interfaces feature introduced on the Cisco CMTS from Cisco IOS Release 12.2(33)SCG onwards enables you to differentiate upstream traffic on the cable bundle or sub-bundle interface and set a corresponding 'qos-group'. This 'qos-group' is used at the output WAN interface to classify and set MPLS EXP bits that are different from the ToS and DSCP value of IP packets.

Note The term cable bundle is used to refer to both the cable bundle and sub-bundle interface in this document.

Table below lists the MQC match statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR10012 router.

Table 154: MQC Match Statements Supported on a Cable Bundle Interface of the Cisco uBR10012 Router

Match Statement	Purpose
access-group	Matches access group name or number.
any	Matches any packet.
dscp	Matches differentiated services code point (DSCP) for IPv4.
precedence	Matches precedence for IPv4.
input-interface	Matches interface specification. **Note** This option supports only bundle interface.
ip dcsp	Matches DSCP for IPv4.
ip precedence	Matches precedence for IPv4.
ip rtp	Matches Real-Time Transport Protocol (RTP) port numbers for IPv4.
not	Negates match result.
qos-group	Matches QoS group. **Note** The 'qos-group' is internal to the router and should not be used to classify upstream traffic from external world.

Table below lists the MQC action statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR10012 router.

Table 155: MQC Action Statements Supported on a Cable Bundle Interface of the Cisco uBR10012 Router

Action Statement	Purpose
set dcsp	Sets DCSP value.
set ip dscp	Sets IP DSCP.
set ip precedence	Sets IP precedence.
set precedence	Sets precedence value.
set qos-group	Sets value from 0 to 99.

Table below lists the MQC match statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR7200 series routers.

Table 156: MQC Match Statements Supported on a Cable Bundle Interface of the Cisco uBR7200 Series Routers

Match Statement	Purpose
access-group	Matches access group name.
any	Matches any packet.
class-map	Matches class map name.
discard-class	Discards class identifier.
dscp	Matches DSCP in IPv4 and IPv6 packets.
input-interface	Matches an input interface. **Note** This option supports only the bundle interface.
ip dscp	Matches IP DSCP.
ip precedence	Matches IP precedence.
ip rtp	Matches RTP port numbers.
mpls experimental	Matches MPLS experimental bits.
not	Negates match result.
packet length	Matches layer 3 packet length.
precedence	Matches precedence in IPv4 and IPv6 packets.
protocol	Matches protocol.

Match Statement	Purpose
qos-group	Matches QoS group. **Note** The 'qos-group' is internal to the router and should not be used to classify upstream traffic from external world.
source-address	Matches source address.

Table below lists the MQC action statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR7200 series routers.

Table 157: MQC Action Statements Supported on a Cable Bundle Interface of the Cisco uBR7200 Series Routers

Action Statement	Purpose
set dscp	Sets DSCP value.
set ip dscp	Sets IP DSCP.
set ip precedence	Sets IP precedence value.
set precedence	Sets precedence value.
set qos-group	Sets value from 0 to 99.

How to Configure MQC QoS on the Cisco CMTS Routers

Note MQC support is applicable only to WAN interfaces as DOCSIS has its own QoS mechanism. However, DOCSIS QoS extends limited MQC support for cable interfaces to limit peer-to-peer (P2P) traffic.

This section describes the following required and optional procedures:

Configuring QoS Features Using MQC

To configure QoS features using the Modular QoS CLI, complete the following basic steps:

Step 1 Define a traffic class using the **class-map** command.

Step 2 Create a traffic policy by associating the traffic class with QoS features using the **policy-map** command.

Step 3 Attach the traffic policy to the interface using the **service-policy** command and specify whether the policy has to be applied to inbound or outbound traffic.

What to Do Next

Each of the above-mentioned steps is accomplished using a user interface command. Specifically, the three steps are accomplished through the use of three abstractions, class map, policy map, and service policy.

Note Service policies are applied to Gigabit Ethernet, Ten Gigabit Ethernet, 802.1Q VLAN subinterfaces, and tunnel interfaces. Tunnel interfaces are virtual interfaces without queues, and service policies applied to tunnels cannot contain queuing actions. The Cisco uBR10012 Universal Broadband Router does not support per-subinterface queues for VLAN subinterfaces. However, the VLANs share the main interface queues.

For more information about MQC, see the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmcli2.html Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 document.

Note Though MQC is not broadly supported on cable interfaces as most subscriber queue configuration is controlled by parameters in the cable modem configuration file, a subset of MQC is supported on cable interfaces. This allows multiple service operators (MSOs) to classify P2P traffic based on type of service (ToS) bits and send it to a shaped queue. The P2P traffic control feature can configure shape and queue-limit actions on the P2P traffic control policy map. The ToS P2P is supported only on legacy cable interfaces and not on Wideband or modular cable (MC) interfaces.

Configuring QoS Traffic Classes

The **class-map** command is used to create a traffic class. A traffic class contains three major elements: a name, a series of **match** commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands.

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands; if a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

For more information about the default traffic class, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 document.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** [**match-all** | **match-any**] *class-name* **Example:** `Router(config)# class-map class1`	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class. • **match-all—**(Optional) Specifies that all match criteria in the class map must be matched, using a logical AND of all matching statements defined under the class. This is the default. • **match-any—**(Optional) Specifies that one or more match criteria must match, using a logical OR of all matching statements defined under the class. • *class-name* **—**User-defined name of the class.
Step 4	**match** *type* **Example:** `Router(config-cmap)# match access-group 101`	Specifies the matching criterion to be applied to the traffic, where *type* represents one of the forms of the **match** command.
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

What to Do Next

Table below lists the match options supported on the class-map command.

Table 158: Match Options Supported on the MQC QoS

Command	Purpose
match access-group {*number* | *name*}	Specifies that the packet must be permitted by the specified access control list (ACL). • *number***—**ACL identifier applied to an interface. Valid values are from 1 to 2699. • *name***—**Packet with the indicated name must be permitted by the access list. The name can be a maximum of 40 alphanumeric characters.

Command	Purpose
match-all	Specifies that the packet must match all of the matching criteria defined for a class map.
match-any	Specifies that the packet must match at least one of the matching criteria defined for a class map.
match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]	Specifies that the packet must match on the basis of a Layer 2 CoS/Inter-Switch Link (ISL) marking. • *cos-value*— IEEE 802.1Q/ISL CoS value. The cos-value can range from 0 to 7; up to four CoS values, separated by a space, can be specified in one match cos statement.
match input-interface *name*	Specifies that the packet input interface must match the interface name. **Note** Matching is supported for cable bundles but not for physical cable interfaces.
match ip dscp {*ip-dscp-value* | **afxy** | **csx** | **ef** | **default**}	Specifies that the packet IP differentiated service code point (DSCP) value must match one or more of the specified attributes. • *ip-dscp-value*—*DSCP* value to match. Valid values are from 0 to 63. You can specify up to 8 code point values, using a space to separate consecutive values. Instead of specifying a numeric ip-dscp-value, you can specify one of the following reserved keywords: • **afxy**—Indicates assured forwarding points. The first number (x) indicates the AF class. Valid values are from 1 to 4. The second number (y) indicates the level of drop preference within each class. Valid values are from 1 (low drop) to 3 (high drop). • **csx**—Indicates class selector code points that are backward-compatible with IP precedence. Valid values for x are from 1 to 7. The CS code points (CS1 through CS7) are identical to IP precedence values from 1 to 7. • **ef**—Indicates expedited forwarding. • **default**—Indicates best effort or DSCP 0.

Command	Purpose
match ip precedence {*ip-precedence-value* | *precedence-name*}	Specifies that the packet IP precedence value must match one or more precedence values or the name of the precedence. • *ip-precedence-value* —IP precedence value to match. Valid values are from 0 to 7. You can specify up to 8 precedence values, using a space to separate consecutive values. • *precedence-name*—Name of the IP precedence value.
match ip rtp {*lowest-udp-port range* }	Specifies that the packet with even-numbered UDP port value must be within the specified range of port numbers. Only even-numbered ports are matched because they carry the real-time data streams. Odd-numbered ports are not matched because they only carry control information. • *lowest-udp-port*—Number specified from 0 to 65535 and is the lowest number in the range. • *range*—Number specified from 0 to 65535 and is the highest number in the range.
match mpls experimental topmost *value*	Matches the experimental (EXP) value in the topmost label. • *value*—Value to which you want to set the MPLS EXP bits in the topmost label header. Valid values are from 0 to 7.
match not *criteria*	Specifies that the packet must not match this particular matching criterion value. • *criteria*—Match criterion value that should be an unsuccessful match criteria. All other values of the specified match criterion are considered successful match criteria.
match qos-group *number*	Specifies that the packet QoS group number value must match the specified QoS group number. • *number*—Group number specified from 0 to 99.

Configuring Traffic Policies

After creating traffic classes, you can configure traffic policies to configure marking features to apply certain actions to the selected traffic in those classes.

The **policy-map** command is used to create a traffic policy. The purpose of a traffic policy is to configure the QoS features that should be associated with the traffic that has been classified in a user-specified traffic class.

Note A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy will be used.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map***policy-map-name* **Example:** `Router(config)# policy-map policy9`	Creates or modifies a traffic policy and enters policy map configuration mode, where: • *policy-map-name*—Name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class1`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode: • *class-name*—Policy applied to a user-defined class name previously configured. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	end **Example:** `Router(config-pmap)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Defining QoS Actions in a Policy Map

Action commands can be added from within class mode on a policy map. Action commands fall into three general categories as given below:

Set Actions

Set commands allow traffic to be marked such that other network devices along the forwarding path can quickly determine the proper class of service to apply to a traffic flow. Set commands can be applied to both input and output policy maps.

Table below lists the set options supported on the Cisco uBR10012 Universal Broadband Router.

Table 159: Set Options Supported on the MQC QoS

Command	Purpose
set cos {*cos-value* | *from-field* [**table** *table-map-name*]}	Sets the Layer 2 CoS value of an outgoing packet. • *cos-value*—IEEE 802.1Q CoS value. The valid range is from 0 to 7. • *from-field*—Packet-marking category used to set packet CoS value. If a table map is used for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are precedence and dscp. • **table**—(Optional) Sets the values specified in a table that is used to set the CoS value. • *table-map-name*—(Optional) Name of the table map used to specify the CoS value. Maximum of 64 alphanumeric characters.

Command	Purpose
set ip dscp {*ip-dscp-value* | **afxy** | **csx** | **ef** | **default**}	Marks a packet with the differentiated services code point (DSCP) you specify. Valid values are from 0 to 63. Instead of specifying a numeric ip-dscp-value, you can specify one of the following reserved keywords: • **afxy—**Indicates assured forwarding points. The first number (x) indicates the AF class. Valid values are from 1 to 4. The second number (y) indicates the level of drop preference within each class. Valid values are from 1 (low drop) to 3 (high drop). • **csx—**Indicates class selector code points that are backward-compatible with IP precedence. Valid values for x are from 1 to 7. The CS code points (CS1 through CS7) are identical to IP precedence values from 1 to 7. • **ef—**Indicates expedited forwarding. • **default—**Indicates best effort or DSCP 0.
set ip precedence {*precedence-value* }	Marks a packet with the IP precedence level you specify. Valid values are from 0 to 7.
set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}	Set the MPLS EXP field value in the topmost label on either an input or an output interface. • *mpls-exp-value***—**Value used to set the MPLS EXP bits defined by the policy map. The valid values range from 0 to 7. • **qos-group—**Specifies that the qos-group packet-marking category is used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. • **table—**(Optional) Used in conjunction with the **qos-group** keyword. Indicates that the values set in a specified table map will be used to set the MPLS EXP value. • *table-map-name* **—**(Optional) Name of the table map used to specify the MPLS EXP value. Used in conjunction with the table keyword. The name can be a maximum of 64 alphanumeric characters.

Command	Purpose
set qos group *group-id*	Marks a packet with the QoS group identifier you specify. The valid values range from 0 to 99.

Police Actions

Traffic policing is a traffic regulation mechanism that is used to limit the rate of traffic streams. Policing allows you to control the maximum rate of traffic sent or received on an interface. Policing propagates bursts of traffic and is applied to the inbound or outbound traffic on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. Although policing does not buffer excess traffic, in the output direction, a configured queuing mechanism applies to conforming packets that might need to be queued while waiting to be serialized at the physical interface.

Traffic policing uses a token bucket algorithm to manage the maximum rate of traffic. This algorithm is used to define the maximum rate of traffic allowed on an interface at a given moment in time. The algorithm puts tokens into the bucket at a certain rate. Each token is permission for the source to send a specific number of bits into the network. With policing, the token bucket determines whether a packet exceeds or conforms to the applied rate. In either case, policing implements the action you configure such as setting the IP precedence or differentiated services code point (DSCP).

To configure traffic policing based on bits per second, use the **police** command in policy-map class configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** [**name**] **Example:** `Router(config)# policy-map policy9`	Specifies the traffic policy and enters policy-map configuration mode.
Step 4	**class** [**name**] **Example:** `Router(config-pmap)# class class1`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode.

	Command or Action	Purpose
Step 5	police [bps] [burst-normal] [burst-excess] conform [conform-action] exceed [exceed-action] **Example:** `Router(config-pmap-c)# police 10000000 15000 20000 conform transmit exceed drop`	Configures traffic policing based on bits per second. • *bps*—(Optional) Average rate in bits per second (bps). Valid values are from 8,000 to 2,488,320,000 bps. If you only specify police bps, the router transmits the traffic that conforms to the bps value and drops the traffic that exceeds the bps value. • *burst-normal*—(Optional) Normal or committed burst size used by the first token bucket for policing. The burst-normal option specifies the committed burst in bytes. Valid values are from 1 to 512,000,000. The default is 9,216 bytes. • *burst-excess*—(Optional) Excess burst size used by the second token bucket for policing. The burst-excess option specifies the excess burst in bytes. Valid values are from 0 to 1,024,000,000 bytes. The default is 0. You must specify burst-normal before you specify burst-excess. **Note** When the burst-excess value equals 0, we recommend that you set the egress burst-normal value to be greater than or equal to the ingress burst-normal value plus 1. Otherwise, packet loss can occur. For example: burst-excess = 0; egress burst-normal >= ingress burst-normal + 1. • *conform-action*—Action to take on packets that conform to the rate limit. The default action is transmit. You must specify burst-excess before you specify conform. • *exceed-action* —Action to take on packets that exceed the rate limit. The default action is drop. You must specify conform before you specify exceed.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Queuing Actions

When queuing actions are applied to a given class within a policy map, they either cause queues to be created for that particular class of traffic or control how the queues are managed. Queuing commands are valid only in the output direction.

The Cisco uBR10012 Universal Broadband Router supports the MQC policy maps for class queue creation on WAN interfaces.

The following two types of queues are supported through MQC:

- Priority queues—Used mainly for voice traffic. They are policed at their individual committed information rate (CIR) to limit their bandwidth to the subscribed level. Only one priority queue is allowed per logical interface.

- Class queues—Implemented as best effort queues. They are based on a specified bandwidth in Kbps and shaped using the "bandwidth" policy map action. Generally, the specified bandwidth is not guaranteed.

Weighted random early detection (WRED) is a mechanism for controlling congestion of queues. WRED combines the capabilities of the random early detection (RED) mechanism with IP precedence, DSCP, and discard class to provide preferential handling of higher priority packets. For additional information on WRED, refer to the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 .

Note Cisco IOS Release 12.2(33)SCB does not support random-detect for type of service (ToS) peer-to-peer (P2P) policy maps.

Table below lists the **queuing actions** supported on the Cisco uBR10012 Universal Broadband Router.

Table 160: Queuing Actions Supported on the MQC QoS

Command	Purpose
priority	Assigns priority to the class you specified and reserves a priority queue for class-based weighted fair queuing (CBWFQ) traffic. The **priority** command does not have any arguments. You must use the **police** command to specify a guaranteed bandwidth.
queue-limit number-of-packets	Specifies or modifies the maximum number of packets that a particular class queue can hold.
random-detect dscp-based	Configures WRED to drop packets based on a DSCP value.
random-detect precedence-based	Configures WRED to drop packets based on an IP precedence value.

Command	Purpose
random-detect dscp dscp-values sub-class-val1 [...[sub-class-val8]]minimum-thresh *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*	Configures the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value. • dscp-values—DSCP value. The DSCP value can be a number from 0 to 63. • **min-thresh-value**—Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. • **max-thresh-value**—Maximum threshold in number of packets. The value range of this argument is from the value of the **min-thresh-value** argument to 4096. • **max-prob-value**—Specifies the fraction of packets dropped when the average queue depth is at the maximum threshold.
random-detect precedence values *sub-class-val1* [...[*sub-class-val8*]] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*	Configures WRED and distributed WRED (DWRED) parameters for a particular IP Precedence. Valid values are from 0 to 7. Typically, 0 represents low priority traffic that can be aggressively managed (dropped) and 7 represents high priority traffic. • *min-thresh-value*—Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. • *max-thresh-value*—Maximum threshold in number of packets. The value range of this argument is from the value of the min-thresh-value argument to 4096. • *mark-prob-value* —Fraction of packets dropped when the average queue depth is at the maximum threshold.
shape [**average**]*cir*	Shapes traffic to the rate you specify, or shapes traffic based on the percentage of available bandwidth you specify. • **average**—Specifies the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. • *cir*—Committed information rate (CIR), in bits per second (bps).

Command	Purpose
bandwidth {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*}	Specifies or modifies the minimum bandwidth allocated for a traffic class in a policy map. • *bandwidth-kbps*—Minimum bandwidth allocated for a class belonging to a policy map. Accepted input values are from 8 to 10,000,000,000 although the maximum value entered should not be larger than the link bandwidth of the slowest interface to which the policy will be applied. • **percent** *percentage*—Specifies or modifies the minimum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 100. • **remaining percent** *percentage*—Specifies or modifies the minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 100. **Note** Configure the amount of bandwidth large enough to also accommodate Layer 2 overhead.

Attaching Service Policies

The **service-policy** command is used to attach the traffic policy, as specified with the **policy-map** command, to an interface. Because the elements of the traffic policy can be applied to packets entering and leaving the interface, it is essential to specify whether the traffic policy characteristics should be applied to incoming or outgoing packets.

To attach a policy map that the router can use to apply QoS policies to inbound and outbound packets, use the **service-policy** command in interface or map class configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet 3/0/0`	Specifies the interface and enters interface configuration mode.
Step 4	Router(config-if)# service-**policy** {*input* | *output*} *policy-map-name* **Example:** `Router(config-if)# service-policy output policy1`	Specifies a policy map that the router can use to apply QoS policies to inbound or outbound packets. • *input* —Applies the QoS policy to inbound packets. • *output*—Applies the QoS policy to outbound packets. • *policy-map-name*—Name of the policy map (created using the policy-map command) you want to attach. The policy-map-name can be a maximum of 40 alphanumeric characters.

Configuring Output Rate

To restrict the WAN interface bandwidth output rate to a smaller value than that of the physical link bandwidth, use the output-rate command in interface configuration mode.

Note The output-rate command is valid only for Gigabit Ethernet interfaces.

Note Starting with Cisco IOS Release 12.2(33)SCG, the **output-rate** command is not supported and the value 10,000 is used for the output line rate on a Cisco uBR10012 router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface interface-name** **Example:** `Router(config)# interface GigabitEthernet 3/0/0`	Specifies the interface and enters interface configuration mode.
Step 4	**output-rate** *rate* **Example:** `Router(config-if)# output-rate 100`	Specifies a custom-defined output rate to a WAN interface instead of the default line rate. • *rate* —Output rate defined for the WAN interface, in kilobits per second. Valid values range from 1 to 1,000,000.
Step 5	exit **Example:** `Router(config-if)# exit`	Exits the interface configuration mode and returns to privileged EXEC mode.

Configuring Input MQC Support on the Cable Bundle Interfaces

To configure input MQC on a cable bundle interface to differentiate upstream traffic and set corresponding "qos-group" features, follow the steps given below.

Restriction

- QoS actions like policing, shaping, WRED, and queuing are not supported.
- Input MQC cannot be configured on cable physical interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**class-map match-all** *class-name* **Example:** `Router(config)# class-map match-all class-ip-prec-6`	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class. • **match-all—**Specifies that all match criteria in the class map must be matched, using a logical AND of all matching statements defined under the class. This is the default option. • *class-name*—User-defined name of the class.
Step 4	**match ip precedence** *ip-precedence-value* **Example:** `Router(config-cmap)# match ip precedence 6`	Specifies the IP precedence values as match criteria. • *ip-precedence-value* —IP precedence value. The valid values range from 0 to 7.
Step 5	exit **Example:** `Router(config-cmap)# exit`	Exits the class-map configuration mode and returns to global configuration mode.
Step 6	Repeat Step 3, on page 1489 and Step 4, on page 1489 to define the second class map.	
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy-input`	Creates a policy map that can be attached to one or more interfaces to specify a service policy and enters policy map configuration mode. • *policy-map-name* —Name of the policy map. The name can be up to 40 alphanumeric characters.
Step 8	**class** *class-name* **Example:** `Router(config-pmap-c)# class class-ip-prec-6`	Specifies the name of the class for which to create a policy and enters the policy-map class configuration mode. • *class-name*—Name of the class to configure.
Step 9	**set qos-group** *group-id* **Example:** `Router(config-pmap-c)# set qos-group 6`	Sets a group ID that can be used later releases to classify packets. • *group-id*—Group identifier number. The valid range is from 0 to 99.
Step 10	exit **Example:** `Router(config-pmap-c)# exit`	Exits the policy-map class configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 11	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 1`	Configures a cable bundle interface and enters interface configuration mode. • *bundle-number* —Cable bundle interface identification number.
Step 12	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input policy-input`	Attaches a policy map to an input interface that is used as the service policy for the interface • *input* —Attaches the specified policy map to the input interface. • *policy-map-name* —Name of the service policy map (created using the **policy-map** command) to be attached. The name can be up to 40 alphanumeric characters
Step 13	end **Example:** `Router(config-pmap-c)# end`	Exits the interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for MQC QoS

This section provides the following configuration examples:

Example: Configuring the Traffic Class

The following example shows how to create two traffic classes and specify their match criteria. For the first traffic class called class1, access control list (ACL) 101 is used as the match criteria. For the second traffic class called class2, ACL 102 is used as the match criteria. Packets are checked against the contents of these ACLs to determine if they belong to the class.

```
Router(config)# class-map class1

Router(config-cmap)# match access-group 101
Router(config-cmap)# exit

Router(config)# class-map class2

Router(config-cmap)# match access-group 102

Router(config-cmap)# exit
```

Example: Configuring the Traffic Policy

The following example shows how to define a traffic policy called policy1 that contains policy specifications for class1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 3000

Router(config-pmap-c)# queue-limit 30

Router(config-pmap)# exit
```

Example: Attaching the Service Policy

The following example shows how to attach an existing traffic policy to an interface. After you define a traffic policy with the **policy-map** command, you can attach it to one or more interfaces by using the **service-policy** command in interface configuration mode. Although you can assign the same traffic policy to multiple interfaces, each interface can have only one traffic policy attached at the input and only one traffic policy attached at the output.

```
Router(config)# interface GigabitEthernet 3/0/0
Router(config-if)# service-policy output policy1

Router(config-if)# exit
```

Example: Verifying QoS Policy

The following example shows how to verify a policy map configuration by entering any of the following commands in privileged EXEC mode.

```
Router# show policy-map policy-map-name class class-name
Class foobar
      bandwidth percent 20
       packet-based wred, exponential weight 9
      random-detect aggregate
      random-detect precedence values 2 minimum-thresh 1024 maximum-thresh 20481
```

Example: Configuring Input MQC Support on the Cable Bundle Interfaces

The following example shows how to differentiate upstream traffic on the cable bundle interfaces and set corresponding “qos-group” features.

```
!Define two different class maps.
class-map match-all class-ip-prec-6
  match ip precedence 6
class-map match-all class-ip-prec-7
  match ip precedence 7
!Define a policy map.
policy-map policy-input
  class class-ip-prec-6
   set qos-group 6
  class class-ip-prec-7
   set qos-group 7
!Attach the policy map to the cable bundle interface in the input direction.
configure terminal
```

```
interface bundle 1
 service-policy input policy-input
```

How to Configure 802.1p CoS and MPLS EXP on the Cisco CMTS Routers

This section describes the following required procedures:

Configuring 802.1p CoS Matching

Use the following procedure to specify a class-map and match a packet based on the CoS marking.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name*— **Example:** `Router(config)# class-map cos1`	Specifies the class name used for the class in the policy map. • *class-map-name*— Name of the class for the class map.
Step 4	**match cos***cos-value* **Example:** `Router(config-cmap)# match cos 0`	Enters the class-map configuration mode and specifies the class of service that needs to match the class map. • *cos-value*— Packet CoS bit value. The valid values range from 0 to 7. You can specify up to four CoS values in one **match cos** statement.
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

Configuring 802.1p CoS Marking

Use the following procedure to specify a policy-map and associate a map class with it to set the CoS value for an outgoing packet.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map policy-map-name** **Example:** `Router(config)# policy-map cos0`	Specifies a policy map name. • *policy-map-name*—Policy map name.
Step 4	**class name** **Example:** `Router(config-pmap)# class cos1`	Enters the policy-map configuration mode and specifies the map class to which the packets has to be matched. • *name* —Map class name.
Step 5	set cos *cos-value* **Example:** `Router(config-pmap-c)# set cos 2`	Enters the policy-map class configuration mode and specifies a CoS value to associate with the packet. • *cos-value*—Class of service value. The valid values range from 0 to 7.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Configuring MPLS EXP Matching

Use the following procedure to specify a class-map and match a packet based on the EXP marking.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name* **Example:** `Router(config)# class-map exp7`	Specifies the class name used for the class in the policy map. • *class-map-name*—Name of the class for the class map.
Step 4	**match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match mpls experimental topmost 2`	Enters the class-map configuration mode and specifies the MPLS EXP field in the topmost label header. • *number*—MPLS EXP field number. The valid values range from 0 to 7.
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

Configuring MPLS EXP Marking

Use the following procedure to specify a policy-map and associate a map class set to the EXP value for an outgoing packet.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map exp5`	Specifies a policy map name. • *policy-map-name*—Policy map name.
Step 4	**class name** **Example:** `Router(config-pmap)# class exp7`	Enters the policy-map configuration mode and specifies the map class to which the packets has to be matched. • *name*— Map class name.
Step 5	t **set mpls experimental topmos***number* **Example:** `Router(config-pmap-c)# set mpls experimental topmost 2`	Enters the policy-map class configuration mode and sets the MPLS EXP field in the topmost label header. • *number* —MPLS EXP field number. The valid values range from 0 to 7.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for 802.1p CoS and MPLS EXP Matching and Marking

This section provides the following configuration examples:

Example: Configuring 802.1p CoS Matching

The following example shows how to match traffic classes within the 802.1p domain using packet CoS values.

```
Router> enable
Router# configure terminal
Router(config)# class-map cos1
Router(config-cmap)# match cos 0
Router(config-cmap)# end
```

Example: Configuring 802.1p CoS Marking

The following example shows how to define traffic classes within the 802.1p domain using packet CoS values.

```
Router> enable
Router# configure terminal
Router(config)# policy-map cos2
Router(config-pmap)# class cos1
Router(config-pmap)# set cos 2
Router(config-pmap)# end
```

Example: Configuring MPLS EXP Matching

The following example shows how to match traffic classes within the MPLS domain using packet EXP values.

```
Router> enable
Router# configure terminal
Router(config)# class-map exp1
Router(config-cmap)# match mpls experimental topmost 2
Router(config-cmap)# end
```

Example: Configuring MPLS EXP Marking

The following example shows how to define traffic classes within the MPLS domain using packet EXP values.

```
Router> enable
Router# configure terminal
Router(config)# policy-map exp2
Router(config-pmap)# class exp1
Router(config-pmap)# set mpls experimental topmost 2
Router(config-pmap)# end
```

Verifying 802.1p CoS and MPLS EXP Matching and Marking

This section explains how to verify 802.1p CoS and MPLS EXP configurations on the Cisco CMTS router:

Example: Verifying Matching and Marking

The following example shows how to verify the matching and marking configuration by entering the following command in privileged EXEC mode:

```
Router# ping vrf vrfa 1.3.99.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.3.99.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/20 ms
```

Example: Verifying QoS and Service Flow

The following example shows how to verify the QoS and service flow information for a particular cable modem (CM) by entering the following command in privileged EXEC mode:

```
Router# show cable modem 1.3.99.98 qos
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:01:41.873 pst Thu Mar 3 2011
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
49    US  act   31    BE     7    300000000   1000000     0           1968000
50    DS  act   N/A   BE     0    300000000   3044        0           1969253
```

Example: Verifying Input and Output Service Policies

The following example shows how to verify the statistics and the configurations of the input and output service policies that are attached to an interface by entering the following command in privileged EXEC mode:

```
Router# show policy-map interface gigabitEthernet 1/2/0
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011
 GigabitEthernet1/2/0
  Service-policy input: policy-in
    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
      QoS Set
        precedence 3
          Packets marked 6647740
    Class-map: class-default (match-any)
      1386487 packets, 1903797872 bytes
      30 second offered rate 658000 bps, drop rate 0 bps
      Match: any
  Service-policy output: policy-out
    Class-map: class-pre-1 (match-all)
      2041355 packets, 2857897000 bytes
      30 second offered rate 986000 bps, drop rate 0 bps
      Match: ip precedence 1
      QoS Set
        mpls experimental topmost 1
          Packets marked 2041355
    Class-map: class-default (match-any)
      6129975 packets, 8575183331 bytes
      30 second offered rate 2960000 bps, drop rate 0 bps
      Match: any
```

Example: Verifying PXF QoS

The following example shows how to verify the Parallel eXpress Forwarding (PXF) CPU statistics and QoS for a particular interface by entering the following command in privileged EXEC mode:

```
Router# show pxf cpu statistics qos gigabitEthernet 1/2/0
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:04:11.893 pst Thu Mar 3 2011
   Classmap           Match         Pkts           Bytes
    Index             Number        Matched        Matched
--------------- --------------- --------------- -------------
 policy-in (Input) service-policy :
class-exp-0     (0)     0               6674330         751960948
class-default   (1)     0               1392134         1911548970
 policy-out (Output) service-policy :
class-pre-1     (0)     0               2049682         2869554800
class-default   (1)     0               6154976         20224030
```

Example: Verifying MPLS Virtual Circuits

The following example shows how to verify the state of all virtual circuits associated with an MPLS pseudowire by entering the following command in privileged EXEC mode:

```
Router# show cable l2-vpn xconnect mpls-vc-map state
Load for five secs: 2%/0%; one minute: 2%; five minutes: 1%
Time source is hardware calendar, *23:05:30.061 pst Thu Mar 3 2011
MAC Address    Peer IP Address  VCID  Type  Prio  State  Customer Name/VPNID  State
54d4.6f88.7362  10.8.8.8        97    Prim*        UP                          UP
```

Example: Verifying MPLS Mapping

The following example shows how to verify the details about the mapping between an MPLS pseudowire and its virtual circuits by entering the following command in privileged EXEC mode:

```
Router# show cable l2-vpn xconnect mpls-vc-map 54d4.6f88.7362 verbose
Load for five secs: 2%/0%; one minute: 1%; five minutes: 2%
Time source is hardware calendar, *16:46:29.139 pst Thu Mar 3 2011
MAC Address                          : 54d4.6f88.7362
Customer Name                        :
Prim Sid                             : 18
Cable Interface                      : Cable5/0/1
MPLS-EXP                             : 0
PW TYPE                              : Ethernet
Backup enable delay                  : 0 seconds
Backup disable delay                 : 0 seconds
Primary peer
Peer IP Address (Active)             : 10.8.8.8
XConnect VCID                        : 97
Circuit  ID                          : Bu254:97
Local State                          : UP
Remote State                         : UP
Total US pkts                        : 418756
Total US bytes                       : 586227332
Total US pkts   discards             : 0
Total US bytes  discards             : 0
Total DS pkts                        : 417347
Total DS bytes                       : 591773612
Total DS pkts   discards             : 0
Total DS bytes  discards             : 0
```

Additional References

The following sections provide references related to the MQC QoS feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Modular Quality of Service Command-Line Interface	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
IP Differentiated Services Code Point Marking	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
Weighted Random Early Detection	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
DiffServ Tunneling Modes for MPLS Networks	MPLS Design TechNotes

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MQC QoS on the Cisco CMTS Routers

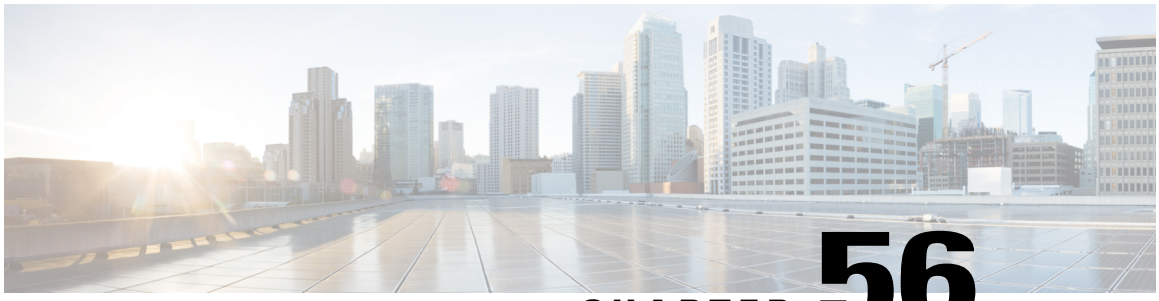
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 161: Feature Information for MQC QoS on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
MQC QoS on the Cisco CMTS Routers	12.2(33)SCB	MQC simplifies the configuration of QoS on the Cisco CMTS routers by defining a common command syntax and resulting set of QoS behaviors across platforms.
MQC QoS on the Cisco CMTS Routers	12.2(33)SCC	The output-rate command was introduced to limit the upstream bandwidth output rate to a smaller number than that of the physical link bandwidth.
802.1Q QoS Support on GiGE WAN	12.2(33)SCF	This feature introduces QoS service on the Gigabit Ethernet WAN interface for 802.1q packets, enabling the user to set priority bits for traffic prioritization. The following commands were introduced or modified: • **class** • **class-map** • **policy-map** • **match cos** • **set cos**

Feature Name	Releases	Feature Information
MPLS short-pipe mode	12.2(33)SCF	This feature introduces QoS service on the WAN interface for MPLS EXP bits, enabling the user to set priority bits for traffic prioritization. The following commands were introduced or modified: • **match mpls experimental topmost** • **set mpls experimental topmost** • **show policy-map interface** • **show cable l2-vpn xconnect**
Input MQC Support on the Cable Interfaces	12.2(33)SCG	This feature enables you to differentiate upstream traffic on cable bundle interface and set MPLS EXP bits without changing the ToS and DSCP value of IP packets. The following sections provide information about this feature: • Input MQC Support on the Cable Bundle Interfaces , on page 1472 • Configuring Input MQC Support on the Cable Bundle Interfaces, on page 1488 • Example: Configuring Input MQC Support on the Cable Bundle Interfaces, on page 1491



CHAPTER 56

Service Flow Admission Control for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the topics, advantages, configuration, and monitoring capabilities of Service Flow Admission Control (SFAC) on the Cisco CMTS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

- Feature Information for SFAC for the Cisco Cable Modem Termination System, page 1542

Prerequisites for SFAC for the Cisco CMTS Routers

The Service Flow Admission Control (SFAC) feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Table below shows the hardware compatibility prerequisites for this feature.

Table 162: SFAC Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCA and later releases • PRE-2 Cisco IOS Release 12.2(33)SCB and later releases • PRE-4 Cisco IOS Release 12.2(33)SCC and later releases • PRE-2 • PRE-4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR10-MC5X20S/U/H • Cisco uBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [106]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR7246VXR Universal Broadband Router only • NPE-G1 • NPE-G2 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[107] **Note** Cisco uBR-MC88V is supported only on Cisco IOS Release 12.2(33)SCD and later releases.
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

106 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

107 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for SFAC

SFAC in Cisco IOS Release 12.3(21)BC and 12.2(33)SC follows these general factors when implementing on the Cisco CMTS:

- Configure SFAC before admitting any static or dynamic service flows. The best option is to have the configuration in place during startup time, or before the interface is up.
- SFAC in Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SC supports the following resource monitoring on the Cisco CMTS:

- Upstream and downstream bandwidth on the Cisco CMTS
- CPU utilization and memory resources on the Cisco uBR10012, Cisco uBR7246VXR, and Cisco uBR7225VXR router chassis (Cisco uBR10-MC5X20U and Cisco uBR-MC88V broadband processing engines)

- SFAC does not support WAN bandwidth monitoring for the Cisco uBR10012, Cisco uBR7246VXR, and Cisco uBR7225VXR routers.

Information About SFAC

This section describes DOCSIS topics and configuration options supported on the Cisco CMTS for SFAC.

Overview of SFAC for the Cisco CMTS

SFAC on the Cisco CMTS is a mechanism that gracefully manages service flow admission requests when one or more resources are not available to process and support the incoming service request. Lack of such a mechanism not only causes the new request to fail with unexpected behavior but could potentially cause the flows that are in progress to have quality related problems. SFAC monitors such resources constantly, and accepts or denies requests depending on the resource availability.

SFAC enables you to provide a reasonable guarantee about the Quality of Service (QoS) to subscribers at the time of call admission, and to enable graceful degradation of services when resource consumption approaches critical levels. SFAC reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

SFAC 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, SFAC verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

SFAC 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. SFAC checks are performed before the flow is admitted.

SFAC in Cisco IOS Release 12.3(21)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization* —SFAC 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)* —SFAC monitors one or both memory resources and their consumption, and preserves QoS in the same way as with CPU utilization.
- *Bandwidth utilization for upstream and downstream* —SFAC monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Note See also SFAC and Cisco CMTS Resources, on page 1508.

Note SFAC begins graceful degradation of service when either a critical threshold is crossed, or when bandwidth is nearly consumed on the Cisco CMTS, depending on the resource being monitored.

SFAC enables you to configure major and minor thresholds for each resource on the Cisco CMTS. These thresholds are expressed in a percentage of maximum allowable resource utilization. Alarm traps may be sent each time a minor or major threshold is crossed for a given resource.

For system-level resources, such as CPU and memory utilization, you can configure critical thresholds in addition to the major and minor thresholds. When a critical threshold is crossed, further service requests are gracefully declined until the associated resource returns to a lower threshold level.

For upstream (US) and downstream (DS) channels, you can configure the bandwidth allocation with exclusive and non-exclusive thresholds. These thresholds can be configured for specified DOCSIS traffic types.

- Exclusive bandwidth indicates the percentage of bandwidth that is allocated exclusively for the specified traffic type. This bandwidth may not be shared with any other traffic type.
- Non-exclusive bandwidth indicates the percentage of bandwidth that is configured in addition to the exclusive bandwidth. Non-exclusive bandwidth is also configured for specific DOCSIS traffic types. Non-exclusive bandwidth is not guaranteed, and may be shared with other traffic types.
- The sum of exclusive and non-exclusive thresholds indicates the maximum bandwidth the specified traffic type may use.

SFAC and Cisco Universal Broadband Routers

SFAC on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SC support SFAC on the Cisco uBR10012 router and all broadband processing engines.

Starting with Cisco IOS Release 12.2(33) SCC, the SFAC support is extended to bonded channels (wideband interface for downstream and upstream channel bonding), modular cable, and integrated cable interfaces.

SFAC on the Cisco uBR7246VXR and the Cisco uBR7225VXR Universal Broadband Routers

Cisco IOS release 12.3(21)BC and Cisco IOS release 12.2(33)SC support SFAC on the Cisco uBR7246VXRand uBR7225VXR routers.

Starting with Cisco IOS Release 12.2(33) SCC, the SFAC support is extended to bonded channels (wideband interface for downstream and upstream channel bonding), modular cable, and integrated cable interfaces.

interface for down stream and upstreamCB) as well as Modular cable and Integrated cable interfaces.

SFAC and Memory Requirements for the Cisco CMTS

SFAC for the Cisco CMTS is a powerful feature that maintains Quality of Service (QoS) on the Cisco CMTS and enforces graceful degradation in service when attempted consumption exceeds resource availability.

Additional memory is required in the Cisco universal broadband router to maintain and store information about various scheduling types, the distribution of upstream or downstream traffic, and associated resource

check processes. For complete information about memory requirements and Cisco IOS Release 12.3(21)BC, refer to the corresponding release notes for your product:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*

http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

- *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC*

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

- *Release Notes for Cisco Universal Broadband Routers in Cisco IOS Release 12.2SC*

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

SFAC and Cisco CMTS Resources

SFAC with Cisco IOS Release 12.3(21)BC implements graceful QoS policies for the following resources of the Cisco CMTS:

System-Level Resources—Impact All Cisco CMTS Functions

- CPU utilization on route processor or broadband processing engine (BPE) modules
- I/O memory on route processor or broadband processing engine modules
- Processor memory

Bandwidth-Level Resources—Impact Traffic Per Interface or Per Port

- Downstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs
- Upstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs

Cisco IOS release 12.3(21)BC supports the following resources for the following Cisco CMTS routers:

Cisco uBR10012 Router Resources

- Cisco uBR Route Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources with the Cisco MC28U Cable Interface Line Card

- Cisco uBR Route Processor

- CPU Utilization
- Processor Memory
- I/O Memory

- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources without the Cisco MC28U Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources with the Cisco MC88V Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory

- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources without the Cisco MC88V Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources with the Cisco MC28U Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources without the Cisco MC28U Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources with the Cisco MC88V Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources without the Cisco MC88V Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth

- Upstream Bandwidth

For more information, see the How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 1513.

SFAC and CPU Utilization

CPU utilization is defined and monitored either as a five-second or a one-minute average. Both averages cannot be configured at the same time for any given resource. For CPU utilization, you can set minor, major, and critical threshold levels.

For additional information, refer to the Configuring SFAC Based on CPU Utilization, on page 1515.

SFAC and Memory Utilization

SFAC can define up to three different memory options on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory resources are similar to CPU utilization, in that you can set minor, major, and critical threshold levels. Memory-based SFAC is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory.

For additional information, refer to the Configuring SFAC Based on Memory Resources, on page 1516.

SFAC and Upstream or Downstream Bandwidth Utilization

SFAC allows you to control the bandwidth usage for various DOCSIS traffic types or application types. The application types are defined by the user using a CLI to categorize the service flow.

Categorization of Service Flows

The SFAC feature allows you to allocate the bandwidth based on the application types. Flow categorization allows you to partition bandwidth in up to eight application types or buckets. The composition of a bucket is defined by the command-line interface (CLI), as is the definition of rules to categorize service flows into one of these eight application buckets. Various attributes of the service flow may be used to define the rules.

For flows created by PacketCable, the following attributes may be used:

- The priority of the Packetcable gate associated with the flow (high or normal)

For flows created by PacketCable MultiMedia (PCMM), the following attributes may be used:

- Priority of the gate (0 to 7)
- Application type (0 to 65535)

The scheduling type for Upstream flows uses the following attribute type:

- Service class name

Before a service flow is admitted, it is passed through the categorization routine. Various attributes of the service flow are compared with the user-configured rules. Based on the match, the service flow is labeled with application type, from 1 to 8. The bandwidth allocation is then performed per application type.

Before a service flow is admitted, it is categorized based on its attributes. The flow attributes are compared against CLI-configured rules, one bucket at a time. If a match is found for any one of the rules, the service flow is labeled for that bucket, and no further check is performed.

Bucket 1 rules are scanned first and bucket 8 rules are scanned last. If two different rules match two different buckets for the same service flow, the flow gets categorized under the first match. If no match is found, the flow is categorized as Best Effort (BE) and the bucket with best effort rule is labelled to the flow. By default, the BE bucket is bucket 8.

Thresholds for Upstream or Downstream Bandwidth

SFAC monitors upstream or downstream bandwidth consumption with minor, major, and critical thresholds. SFAC generates alarm traps when bandwidth consumption crosses minor and major thresholds. For additional information, refer to the How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 1513.

Exclusive and Non-Exclusive Bandwidth Thresholds

In addition to minor and major thresholds, SFAC also allows configuration of exclusive or non-exclusive thresholds.

- *Exclusive* bandwidth thresholds, for the upstream or downstream bandwidth, define a given percentage of the total (100%) bandwidth, and dedicate it to a specific traffic type.
- *Non-exclusive* bandwidth thresholds can be shared with multiple traffic types. Non-exclusive bandwidth is typically used by Best Effort traffic, yet remains available to other traffic types when required.

When the traffic usage exceeds the exclusive threshold, SFAC checks if there is any non-exclusive bandwidth available. Any new service request is permitted only if sufficient non-exclusive bandwidth is available.

Comparing SFAC with Prior Admission Control

The prior Admission Control feature on the Cisco CMTS was introduced in Cisco IOS Release 12.3(13a)BC. This prior version of Admission Control allows you to set minor, major, exclusive and non-exclusive thresholds. This topic lists changes introduced for SFAC in Cisco IOS Release 12.3(21)BC, and identifies which part of the functionality is changed and which functionality is preserved.

Note The configuration, monitoring, and debugging commands used for the original Admission Control feature are not supported for the SFAC bucket scheme.

- SFAC retains the prior Admission Control concept of thresholds. SFAC enables configuration of major, minor, exclusive and non-exclusive thresholds. However, SFAC is *distinct and unique in that the thresholds are applied per application bucket, numbered 1 to 8.*

- For downstream service flows, the prior Admission Control feature permitted bandwidth allocation for only data and voice traffic, and only PacketCable voice was recognized. SFAC uniquely allows bandwidth allocation per application bucket. As with Admission Control, however, SFAC allocates bandwidth for PacketCable voice by configuring the appropriate rules that apply to the application buckets.
- Upstream bandwidth allocation in SFAC is not based on the scheduling types, such as UGS, RTPS and so forth. SFAC newly handles upstream channels in fashion similar to downstream channels—the upstream channels also support eight application types. You may configure SFAC bandwidth allocation based on the scheduling types. You achieve the same result, however, by defining the appropriate rules to map each scheduling type into one of the eight buckets.
- SFAC monitors and manages Cisco CMTS resources according to the categorization of service flow, in which service flow policies, status and resource management are configured and processed in more categorical fashion, to include support for both PacketCable and PacketCable MultiMedia voice traffic.
- SFAC newly treats upstream and downstream traffic in the same manner and in more uniform fashion than the previous Admission Control feature.
- Exclusive and non-exclusive thresholds define resource management processes of the SFAC feature.
- SFAC introduces enhanced support for the CISCO-CABLE-ADMISSION-CTRL-MIB.

Overview of Bonding Group Admission Control

DOCSIS 3.0 introduced bonded channels or bonding groups that allow a single cable modem to send data over multiple RF channels achieving higher throughput. These bonding groups are defined for both upstream and downstream channels. Cisco IOS 12.2(33)SCC release extends the SFAC feature to support upstream and downstream bonding groups.

Bonding groups are created by combining multiple RF channels. A single RF channel may also be shared by multiple bonding groups.

Bonding group SFAC functionality allows to define the maximum reserved bandwidth for an application-type as a fraction of the available bandwidth. This fraction of the bandwidth is defined as a percentage value of the total bandwidth that can be reserved.

In order to support SFAC for bonding groups, Cisco IOS 12.2(33)SCC release introduced a new command to specify the reserve-able bandwidth available for a bonding group. Thus 100% threshold equals the bandwidth that can be reserved for a bonding group.

For additional information, refer to the Defining Maximum Reserved Bandwidth Limit, on page 1521.

How to Configure, Monitor, and Troubleshoot Service Flow Admission Control

This section describes the following configuration, monitoring and troubleshooting procedures for the SFAC (SFAC) feature. Configuration procedures are optional, given default configurations are enabled in Cisco IOS Release 12.3(21)BC. This section presents a sequence of procedures for non-default configurations, monitoring and debugging procedures that apply in default or non-default operations of SFAC.

Enabling SFAC for Event Types

SFAC can be enabled for one or more of the following events. At least one of these events must be configured for SFAC on the Cisco CMTS prior to the configuration of any additional settings:

- the registration of a cable modem
- the request for a dynamic service, such as a PacketCable or PCMM voice call

Perform these steps to configure either or both event types on the Cisco CMTS.

Note Starting from Cisco IOS Release 12.2(33)SCC, during a CM registration process, if a SFAC committed information rate (CIR) threshold value for a matching bucket is exceeded due to admission of a non-zero CIR service flow, the CM registration will be rejected by admission control with a minimum reserve rate failure. This functionality helps in avoiding CIR over-subscription that was observed in CM registration processes prior to Cisco IOS Release 12.2(33)SCC.

Before You Begin

SFAC requires that event types, traffic types and CMTS resource thresholds be configured and enabled on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable admission-control event** { **cm-registration** | **dynamic-service** } **Example:** `Router(config)# cable admission-control event cm-registration` `Router(config)# cable admission-control event dynamic-service`	Sets the event type on the Cisco CMTS when SFAC performs resource monitoring and management. At least one of the following keywords must be used, and both can be set: • **cm-registration—**Sets SFAC checks to be performed when a cable modem registers. If there are insufficient resources at the time of registration, the cable modem is not allowed to come online. • **dynamic-service—**Sets SFAC checks to be performed when a dynamic service, such as a voice call, is requested. **Note** The Cisco CMTS displays a warning message if any one of the event type is disabled.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Once configured, event types and SFAC event activity on the Cisco CMTS can be reviewed using the following two commands:

- **debug cable admission-control** *options*
- **show cable admission-control**

If the resources to be monitored and managed by SFAC are not yet configured on the Cisco CMTS, refer to the additional procedures in this document for information about their configuration.

Configuring SFAC Based on CPU Utilization

SFAC allows you to configure minor, major and critical thresholds for CPU utilization. The thresholds are specified as percentage of CPU utilization. When the an event such as cable modem registration or dynamic service takes place, and the CPU utilization is greater than the major or minor threshold, an alarm is generated. If it is greater than the critical threshold, the new service is gracefully declined.

SFAC enforces threshold levels in one of two ways. The Cisco CMTS supports both enforcement methods, but both cannot be configured at the same time.

- cpu-5sec—This finest-level setting configures the Cisco CMTS to reject new requests when the cpu-5sec utilization has exceeded the configured critical threshold. This protects any time-sensitive activities on the router. SFAC takes action on the router when a new request might otherwise exceed the configured CPU threshold level.

Note When CPU utilization exceeds the critical threshold, new requests for dynamic service flow creation for packetcable are rejected. However, new requests for CM registration will still be accepted as long as bandwidth thresholds are not crossed.

- cpu-avg—This normal-level setting is a CPU utilization average, enforced by sampling the CPU utilization at much lower frequency and calculating an exponentially weighted average. SFAC takes action on the router when a new service request might otherwise exceed the configured CPU peak threshold level.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	[**no**] **cable admission-control** {**cpu-5sec** | **cpu-avg**} **minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router# no cable admission-control cpu-avg minor 60 major 70 critical 80`	Configures CPU memory thresholds on the Cisco CMTS for SFAC. • **cpu-5sec—**average CPU utilization over a period of five seconds. • **cpu-avg—**average CPU utilization over a period of one minute. • **minor***num1* **—**Specifies the minor threshold level, where *num1* is a percentage and can be an integer between 1 and 100. • **major***num2* **—**Specifies the major threshold level, where *num2* is a percentage and can be an integer between 1 and 100. • **critical***num3* **—**Specifies the critical threshold level, where *num3* is a percentage and can be an integer between 1 and 100. There are no default values for this command. **Note** **cpu-5sec** and **cpu-avg** cannot be configured at the same time.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configured.

Note The minor threshold should be less than the major threshold, and the major threshold must be less than the critical threshold.

Configuring SFAC Based on Memory Resources

Three different memory resource options can be configured on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory-based SFAC is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory. As with CPU utilization, you can set minor, major, and critical threshold levels.

Note When memory utilization exceeds the critical threshold, new requests for dynamic service flow creation for packetcable are rejected. However, new requests for CM registration will still be accepted as long as bandwidth thresholds are not crossed.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **cable admission-control** { **io-mem** | **proc-mem** | **total-memory**} **minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router# no cable admission-control io-mem minor 60 major 70 critical 80`	Configures CPU memory thresholds on the Cisco router. There are no default values for this command. **Note** All three memory threshold levels can and should be configured.
Step 4	Ctrl-Z **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configure.

Defining Rules for Service Flow Categorization

This procedure describes how to configure service flow categorization rules on the Cisco CMTS. This flexible procedure changes default global service flow rules with variations of the **cable application type include** command.

By default, Cisco IOS Release 12.3(21)BC enables the definition of service flows according to application or traffic type, with bucket assignments for a standard set of service flow applications.

Any one or several of these steps or commands may be used, in nearly any combination, to set or re-configure SFAC on the Cisco CMTS.

Note Application rules for SFAC are global configurations, and upstream and downstream bandwidth resources use the same sets of service flow rules.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable application-type** *n* **include packetcable** { **normal** | **priority** } **Example:** `Router(config)# cable application-type 5 include packetcable priority`	For PacketCable, this command variation maps PacketCable service flow attributes to the specified bucket. PacketCable service flows are associated with PacketCable gates. The gate can be normal or high-priority.
Step 4	**cable application-type** *n* **include pcmm** {**priority** *gate-priority* / **app-id** *gate-app-id* } **Example:** `Router(config)# cable application-type 2 include pcmm priority 7` `Router(config)# cable application-type 2 include pcmm app-id 152`	For PCMM, this command variation maps PCMM service flow priority or application to the specified bucket. The PCMM gates are characterized by a priority level and by an application identifier.
Step 5	**cable application-type** *n* **include scheduling-type** *type*	For DOCSIS scheduling types, this command variation binds the DOCSIS scheduling types into the designated application bucket. DOCSIS 1.1 specifies the scheduling type to bind QoS parameters to the service flows for upstream traffic.

	Command or Action	Purpose
	Example: `Router(config)# cable application-type 1 include scheduling-type ugs` `Router(config)# cable application-type 1 include scheduling-type ugs-ad`	
Step 6	**cable application-type** *n* **include service-class** *service-class-name* **Example:** `Router(config)# cable application-type 1 include service-class stream1`	For service class parameters, this command variation applies a service class name to the service flows, and applies corresponding QoS parameters. DOCSIS 1.1 introduced the concept of service classes. A service class is identified by a service class name. A service class name is a string that the Cisco CMTS associates with a QoS parameter set One of the objectives of using a service class is to allow the high level protocols to create service flows with the desired QoS parameter set. Using a service class is a convenient way to bind the application with the service flows. The rules provide a mechanism to implement such binding. Note the following factors when using the command in this step: • Service classes are separately configured using the **cable service class** command to define the service flow. • A named service class may be classified into any application type. • Up to ten service class names may be configured per application types. Attempting to configure more than ten service classes prints an error message. • Use the **no cable traffic-type** command to remove the configuration of a service class before adding a new class.
Step 7	**cable application-type** *n* **include BE** **Example:** `Router# cable application-type 3 include BE`	For Best Effort service flows, this command variation elaborates on Step 3, and changes the default bucket of 8 for Best Effort service flows with non-zero Committed Information Rate (CIR). These BE service flows are often created during cable modem registration. Note that there is an alternate rule that applies to the Best Effort scheduling type. This rule is applicable only for upstream service flows, as described in an earlier step of this procedure. The BE CIR service flow rule may be applicable to both upstream and downstream. However, in the case of upstream service flows, in most cases, the same service flow may map both the rules.
Step 8	Ctrl-Z **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

The following example maps high-priority PacketCable service flows into application bucket 5.

```
Router(config)# cable application-type 5 include packetcable priority
```

The following example maps normal PacketCable service flows into application bucket 1.

```
Router(config)# cable application-type 1 include packetcable normal
```

The following example maps the specified bucket number with PCMM service flow with a priority of 7, then maps an application identifier of 152 for the same bucket number:

```
Router(config)# cable application-type 2 include pcmm priority 7
Router(config)# cable application-type 2 include pcmm app-id 152
```

The following example maps both UGS and UGS-AD into bucket number 1:

```
Router(config)# cable application-type 1 include scheduling-type ugs
Router(config)# cable application-type 1 include scheduling-type ugs-ad
```

The following example maps the Best Effort CIR flows to bucket 3:

```
Router(config)# cable application-type 3 include BE
```

Naming Application Buckets

This procedure enables you to assign alpha-numeric names to six of the eight application buckets that SFAC supports. The default bucket identifiers range from 1 to 8.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable application-type** *n***name** *bucket-name* **Example:** `Router(config)# cable application-type 7 name besteffort`	Assigns an alpha-numeric name for the specified bucket. **Note** This bucket name appears in supporting **show** and **debug** commands along with the default bucket number.
Step 4	Ctrl-Z **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Defining Maximum Reserved Bandwidth Limit

This procedure enables you to define the maximum bandwidth available for CIR reservations per bonding group for all service flows that are allowed by the Cisco CMTS. The bandwidth limit depends on the RF bandwidth percent configuration for the specific bonding group.

The max-reserved-bandwidth for WB/MC/IC interfaces have lower threshold as 1% instead of 0%. For upstream and downstream bonding the lower threshold is 0%.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* } **Example:** `Router(config)# interface cable w1/0/0:0`	(Optional) Interface configuration mode implements this feature only for the specific WB, IC, or MC interface, and upstream bonding groups. Use global configuration mode in step 4 for global configurations. If downstream thresholds are configured for the interface, then that configuration supersedes the global configuration.
Step 4	**cable admission-control max-reserved-bandwidth** *bw-in-kbps* **Example:** `Router(config-if)# cable admission-control max-reserved-bandwidth 6344`	Defines the maximum reserved bandwidth for the specific WB, IC or MC interface.
Step 5	*Ctrl-Z* **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Setting Downstream and Upstream Application Thresholds

This procedure sets downstream and upstream applications thresholds for SFAC on the Cisco CMTS. This procedure extends the previous Admission Control commands from earlier Cisco IOS releases to support additional applications in SFAC. The settings in this procedure may be applied in either global or per-interface mode for downstream and upstream applications, and may also be applied in per-upstream fashion if desired.

Precedence of These Configuration Commands

SFAC based on bandwidth can be configured at the interface or global level. For upstream bandwidth, SFAC can be configured at the per-upstream level as well.

For downstream channels, the interface-level thresholds have higher precedence over the global thresholds configured. For upstream ports, the port-level thresholds have higher precedence over interface-level thresholds; and the interface-level thresholds have higher precedence over global thresholds.

As such, if you configure both global and interface-level downstream thresholds, the interface-level thresholds are effective for that interface. In similar fashion, if you configure port-level settings and the interface-level upstream thresholds, the port-level thresholds are effective on that port. The remaining ports, with no port-level thresholds in place, use the interface-level upstream thresholds.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* } **Example:** `Router(config)# interface c5/0/1` `Router(config-if)#`	(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode in step 4 for global configurations. If downstream thresholds are configured for the interface, then that configuration supersedes global configuration. • *slot* —Slot where the line card resides. ◦ Cisco uBR7225VXR router—The valid range is from 1 to 2. ◦ Cisco uBR7246VXR router—The valid range is from 3 to 6. • *port*—Downstream controller number on the line card. The valid *port* values are 0 or 1. • *slot*/*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router.

	Command or Action	Purpose
		◦ *slot*—Slot where the line card resides. The permitted range is from 5 to 8. ◦ *subslot*—Subslot where the line card resides. The available slots are 0 or 1. ◦ *port*—The downstream controller number on the line card. The permitted *port* range is from 0 to 4.
Step 4	**cable admission-control ds-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25 exclusive 30 non-exclusive 15`	Sets minor, major and exclusive thresholds for downstream voice or data bandwidth for each or all interfaces on the Cisco CMTS. Repeat this step when setting bandwidth for multiple buckets. Global configuration mode implements this feature across the entire Cisco CMTS. Otherwise, use this command in interface configuration mode as per step 3. Bandwidth values are as follows: • **ds-bandwidth**—Sets downstream throughput thresholds. • **bucket-no** *n* —Keyword and variable select the bucket number for which this configuration applies. • n—Selects the application bucket number for which this configuration applies. • **minor** *minor-threshold* —Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage* —Specifies the percentage of throughput reserved exclusively for this class (voice or data). The *exclusive-percentage* value is an integer between 1 and 100. No other bucket can use this throughput. • **non-exclusive***non-exclusive-percentage* —(Optional) Specifies the percentage of throughput, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this throughput is non-exclusive, it can be used by other buckets as specified. **Note** CMTS supports this command on modular cable and integrated cable interfaces. The no form of this command removes downstream bandwidth configuration from the Cisco CMTS: • **nocable admission-control ds-bandwidth**
Step 5	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* } **Example:** `Router(config)# interface c5/0/1` `Router(config-if)#`	(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations. • *slot* —Slot where the line card resides. ◦ Cisco uBR7225VXR router—The valid range is from 1 to 2. ◦ Cisco uBR7246VXR router—The valid range is from 3 to 6.

	Command or Action	Purpose
		• *port*—Downstream controller number on the line card. The valid *port* values are 0 or 1. • *slot* /*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router. ◦ *slot*—Slot where the line card resides. The permitted range is from 5 to 8. ◦ *subslot*—Subslot where the line card resides. The available slots are 0 or 1. ◦ *port*—The downstream controller number on the line card. The permitted *port* range is from 0 to 4.
Step 6	**cable admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds. • **bucket-no** *n* —Selects the application bucket for which this configuration applies.: • **minor** *minor-threshold*—Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage*—Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The exclusive-percentage value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage*—(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified. **Note** CMTS supports this command on modular cable and integrated cable interfaces.
Step 7	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* } **Example:** `Router(config)# interface c5/0/1` `Router(config-if)#`	(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations. If downstream thresholds are configured for the interface, then that configuration supersedes global configuration. • *slot* /*port* —Designates the cable interface on the Cisco uBR7246VXR and Cisco uBR7225VXR routers. • *slot*/*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router.

	Command or Action	Purpose
Step 8	**cable upstream** *n* **admission-control us-bandwidth bucket-no** *n***minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable upstream 1 admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **upstream—**Specifies that this command applies on per-upstream channel basis. • *n* **—**Specifies the upstream channel number. The traffic type takes the same values as the downstream command. • **us-bandwidth—**Specifies that this command is to configure the upstream bandwidth thresholds. • **bucket-no***n* bucket-no *n* **—**Selects the application bucket for which this configuration applies. • **minor** *minor-threshold* **—**Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold* **—**Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage* **—**Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The exclusive-percentage value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage* **—**(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified.
Step 9	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Preempting High-Priority Emergency 911 Calls

You may configure SFAC rules and thresholds so that the high-priority voice (911) traffic receives an exclusive share of bandwidth. Because the average call volume for Emergency 911 traffic may not be very high, the fraction of bandwidth reserved for Emergency 911 calls may be small. In the case of regional emergency, the call volume of Emergency 911 calls may surge. In this case, it may be necessary to preempt some of the normal voice traffic to make room for surging Emergency 911 calls.

The Cisco CMTS software preempts one or more normal-priority voice flows to make room for the high-priority voice flows. SFAC provides the command-line interface (CLI) to enable or disable this preemption ability.

SFAC preemption logic follows the following steps:

1. When the first pass of admission control fails to admit a high priority PacketCable flow, it checks if it is possible to admit the flow in another bucket configured for normal PacketCable calls (applicable only if the PacketCable normal and high-priority rules are configured for different buckets). If the bandwidth is available, the call is admitted in the normal priority bucket.
2. If there is no room in normal priority bucket, it preempts a normal priority PacketCable flow and admits the high priority flow in the bucket where the low priority flow was preempted.
3. If there is no normal priority flow that it can preempt, it rejects the admission for high-priority flow. This usually happens when both normal and high-priority buckets are filled with 911 flows.

This preemption is effective only for PacketCable high-priority flows.

When an upstream or downstream low-priority service flow is chosen for preemption, the corresponding service flow for the same voice call in the opposite direction gets preempted as well.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **cable admission-control preempt priority-voice** **Example:** `Router(config)# no cable admission-control preempt priority-voice`	Changes the default Emergency 911 call preemption functions on the Cisco CMTS, supporting throughput and bandwidth requirements for Emergency 911 calls above all other buckets on the Cisco CMTS. The **no** form of this command disables this preemption, and returns the bucket that supports Emergency 911 calls to default configuration and normal function on the Cisco CMTS.
Step 4	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z` `Router#`	Returns to Privileged EXEC mode.

Calculating Bandwidth Utilization

The SFAC feature maintains a counter for every US and DS channel, and this counter stores the current bandwidth reservation. Whenever a service request is made to create a new service flow, SFAC estimates the bandwidth needed for the new flow, and adds it to the counter. The estimated bandwidth is computed as follows:

- For DS service flows, the required bandwidth is the minimum reservation rate, as specified in the DOCSIS service flow QoS parameters.
- For US flows, the required bandwidth is as follows:
  - For BE flows the required bandwidth is the minimum reservation rate as specified in the DOCSIS service flow QoS parameters.
  - For UGS flows the required bandwidth is grant size times number of grants per second, as per the DOCSIS specification.
  - For RTP and RTPS flows, the required bandwidth is sum of minimum reservation rate as specified in the DOCSIS service flow QoS parameters; and the bandwidth required to schedule the request slots.
  - For UGSAD flows the required bandwidth is sum of bandwidth required for payload (same as UGS flows) and the bandwidth required to schedule to request slots.

In each of the above calculations, SFAC does not account for the PHY overhead. DOCSIS overhead is counted only in the UGS and UGS-AD flows. To estimate the fraction of bandwidth available, the calculation must account for the PHY and DOCSIS overhead, and also the overhead incurred to schedule DOCSIS maintenance messages. SFAC applies a correction factor of 80% to the raw data rate to calculate the total available bandwidth.

Note For the DS and US flow in bonded channels, the maximum reserved bandwidth is the bandwidth defined for the SFAC threshold values. This value is indicated in kbps.

Monitoring and Troubleshooting Commands for SFAC

This section describes the following monitoring and troubleshooting procedures for the SFAC (SFAC) feature.

Bandwidth Validity Checks for SFAC

SFAC is based on and monitors multiple resources on the Cisco CMTS. You can configure major, minor, exclusive and non-exclusive thresholds for various traffic types. To prevent circumstances in which some SFAC configurations are inconsistent, SFAC first validates the attempted configuration, and if an error is found, SFAC prints an error message and the configuration is not set.

Before setting the threshold limits for a given resource on the Cisco CMTS, SFAC configuration should follow these important guidelines to ensure a valid configuration:

1. For the given resource, the minor threshold should be less than the major threshold, and the major threshold should be less than the exclusive or critical threshold. For example, minor threshold at 45%, major threshold at 65%, and critical threshold at 85%.
2. For downstream and upstream bandwidth, the sum of the exclusive thresholds and the maximum configured non-exclusive threshold should be less than 100%. For example, consider US bandwidth configuration for various buckets. If exclusive thresholds for buckets 1-4 were configured at 15% each, this would mean a total of 60% bandwidth is reserved exclusively for these four buckets. This leaves only 40% for any non-exclusive bandwidth. Therefore, in this case, the maximum non-exclusive thresholds that any bucket can have is 40% (100% - 60%), and should be less than 40%.

Implicit Bandwidth

You may choose not to assign any explicit thresholds to certain buckets. In this case, these buckets assume implicit thresholds. In the previous example, if you do not configure any thresholds for buckets 5-8, then those buckets assume implicit thresholds. Because 60% bandwidth is already reserved by buckets 1-4, buckets 5-8 can share the remaining 40% bandwidth. This 40% bandwidth is treated in a non-exclusive manner. This information displays in supporting **show** commands. The implicit bucket bandwidth for WB interface is 0 unlike other cable interface types where the implicit bandwidth is 100%.

If cable application type includes any multicast application ID, then CMTS expects default bucket will not accommodate multicast service flows. If no multicast application type is configured, all the multicast service flows are admitted to the default bucket 8.

Once a bucket is configured for one multicast application ID, all the subsequent multicast application IDs should be mapped to buckets other than bucket 8.

Oversubscription

Oversubscription of a given resource on the Cisco CMTS may be encountered in one of the following ways:

- Consider a situation where voice and data are both given 50% exclusive bandwidth. If a large number of cable modems register with non-zero committed information rate (CIR) service flows, this results in consuming a large fraction of the bandwidth. This situation is called oversubscription.
- Cable modem registration with CM configuration files with CIR flows may result in oversubscription. As explained above, the admission of CIR flows, even though it violates the admission control policy, can result in oversubscription.
- Enabling SFAC events after the service flows are admitted may result in oversubscription. If the SFAC check is not enabled using the cable admission-control dynamic-service command, this can result in service flows being admitted. If the thresholds are configured, the bandwidth usage may exceed its allocated share.
- Dynamically changing the thresholds can result in oversubscription. You can make changes in dynamic fashion to the threshold levels while the flows are already admitted. If the new threshold is lower than the current reservation for a given bucket, that bucket will oversubscribe its share under the new and lower threshold.
- The service flow handling method may result in oversubscription. The amount of bandwidth exceeding the allocated bandwidth is measured as "oversubscribed bandwidth". The oversubscribed bandwidth is displayed in the show cable admission-control commands. While calculating the available bandwidth for the rest of the buckets, the oversubscribed bandwidth is not taken into consideration. We calculate effective bandwidth as follows:

Effective bandwidth = current reservation - oversubscribed bandwidth

For example, referring to the starting scenario with voice and data both given 50% bandwidth, if the data usage reaches 70%, the data bucket oversubscription totals 20%. That is, the effective bandwidth for the data bucket = 70 - 20 = 50%.

Therefore, while calculating the available bandwidth for voice, full 50% bandwidth is considered available. Note that in this example, if you allow voice utilization to reach 50%, the total reservation becomes 120%. At present the Cisco CMTS platforms do not allow total reservation to exceed 100% of the available bandwidth for downstream channels; only upstream channels may exceed 100% reservation.

Displaying Application Buckets for SFAC

Cisco IOS Release 12.3(21)BC introduces the **show application-buckets** command to display default or customized SFAC settings and status on the Cisco CMTS. This command displays the bucket number and bucket name, if the latter is configured, and the associated rules for each bucket. When multiple rules are applied to one bucket, the rules display in order of priority for that bucket.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable application-type** [**bucket-no** *n*] **Example:** `Router# show cable application-buckets 5`	Displays rules for any or all buckets supporting SFAC on the Cisco CMTS. The configured rules for any given bucket are displayed in order of precedence in the Rule field. • **bucket-no***n* —You may specify a specific bucket number on the Cisco CMTS to display parameters for that bucket and no others. Valid range is 1 to 8, or all buckets if no specific bucket is designated.

The following example illustrates sample output of the **show cable application-type** command.

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

What to Do Next

The change made with this procedure is displayed with the **show application-buckets** command.

Displaying Service Flow Reservation Levels

Cisco IOS Release 12.3(21)BC introduces a new command to display service flows, application categorizations, and bandwidth consumption on the Cisco CMTS.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface cable** { *slot* / *port* | *slot* / *subslot* / *port* } **admission-control reservation** { **downstream** | **upstream** *port-no* } **Example:** `Router# show interface cable 5/1/1 admission-control reservation downstream`	Displays service flows, categorizations, and bandwidth consumption on the Cisco CMTS, for the specified interface, and the specified service flow direction. • *slot* —Slot where the line card resides. ◦ Cisco uBR7225VXR router—The valid range is from 1 to 2. ◦ Cisco uBR7246VXR router—The valid range is from 3 to 6. • *port* —Downstream controller number on the line card. The valid *port* values are 0 or 1. • *slot* / *subslot* / *port* —Designates the cable interface on the Cisco uBR10012 router. ◦ *slot* —Slot where the line card resides. The permitted range is from 5 to 8. ◦ *subslot* —Subslot where the line card resides. The available slots are 0 or 1. ◦ *port* —The downstream controller number on the line card. The permitted *port* range is from 0 to 4. • **downstream**—Displays downstream service flow information for the designated cable interface. • **upstream** —Displays upstream service flow information for the designated cable interface. The port number may be specified here for more limited display. • *port-no—Port number to which this destination applies; applicable if the upstream ports are configured for SFAC.*

The following example illustrates sample output and status of the SFAC feature, and the **show interface cable admission-control reservation** { **downstream | upstream** } *port-no* command.

```
Router# show interface cable 5/1/1 admission-control reservation downstream
SfId   Mac Address       Bucket    Bucket Name         State    Current Reserv
4      0000.cad6.f052       8                         act       0
88     0000.cad6.f052       8                         act       2000
```

```
6       0000.cad6.eece       8                         act       0
21      0000.cad6.eece       8                         act       2000
8       0000.cad6.eebe       8                         act       0
24      0000.cad6.eebe       8                         act       2000
10      0000.cadb.30a6       8                         act       0
27      0000.cadb.30a6       8                         act       2000
```

Displaying SFAC Configuration and Status

Cisco IOS Release 12.3(21)BC supports an enhanced command to display service flows, application categorizations, and bandwidth consumption status on the Cisco CMTS. This command also displays DS threshold values, reservations per bucket on a modular cable or interface cable or DS channel bonding.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable admission-control** [**global**] [**interface** *slot/port* | *slot/subslot/port*] [**all**] **Example:** `Router# show cable admission-control interface cable 5/1/1 upstream 0`	Displays the current SFAC configuration and status on the Cisco CMTS, or on a specified interface. • **global—**(Optional) Displays the following information: ◦ Parameters that have been configured for admission control ◦ Number of requests that have crossed minor, major, and critical levels for each resource • **interface** *slot/port* | *slot/subslot/port* Option allows you to display SFAC information for the specified interface or port. This includes the following: ◦ Values for US throughput resources ◦ Values for DS throughput resources ◦ *slot/port* —Designates the cable interface on the Cisco uBR7246VXR and Cisco uBR7225VXR routers. ◦ *slot/subslot/port* —Designates the cable interface on the Cisco uBR10012 router. • **all—**Displays information for all interfaces configured for SFAC on the Cisco CMTS.

The following example illustrates further information for the SFAC feature. This example displays threshold levels and current reservation per bucket, and the oversubscribed bandwidth per bucket. Cisco IOS indicates implicitly calculated threshold with asterisk.

```
Router# show cable admission-control interface cable 5/1/1 upstream 0
Interface  Cable5/1/1
Upstream Bit Rate (bits per second) = 4096000
Resource - Upstream Bandwidth
-----------------------------
Bucket Names  Minor # of  Major # of  Excls # of  Non-Ex Curr. Curr. Conf  # of
No            Level Times Level Times Level Times Level  Resv  Ovrsb Level Rejec
1             5     1312  7     1262  45    0     0      31    0     I    36
2             0     0     0     0     0     0     6*     0     0     I     0
3             0     0     0     0     0     0     6*     0     0     I     0
4             0     0     0     0     0     0     6*     0     0     I     0
5             0     0     0     0     0     0     6*     0     0     I     0
6             0     0     0     0     0     0     6*     0     0     I     0
7             0     0     0     0     0     0     6*     0     0     I     0
8             5     31    7     29    49    11    5      79    25    I     0
```

Debugging SFAC for Different Event Types

Cisco IOS Release 12.3(21)BC supports the debugging of service flow events for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Enabling SFAC for Event Types, on page 1513

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control event** **Example:** `Router# debug cable admission-control event`	Enables event-oriented troubleshooting for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enabling and display of the debug cable admission-control event command.

```
Router# debug cable admission-control event
*Sep 12 23:15:22.867: Entering admission control check on PRE and it's a cm-registration
*Sep 12 23:15:22.867: Admission control event check is TRUE
```

Debugging SFAC for CPU Resources

Cisco IOS Release 12.3(21)BC supports the debugging of CPU resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Configuring SFAC Based on CPU Utilization, on page 1515

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control cpu`	Enables CPU troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates enabling and display of the **debug cable admission-control cpu** command.

```
Router# debug cable admission-control cpu
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

Debugging SFAC for Memory Resources

Cisco IOS Release 12.3(21)BC supports the debugging of memory resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Configuring SFAC Based on Memory Resources, on page 1516

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control memory`	Enables memory troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control memory** command.

```
Router# debug cable admission-control memory
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

Debugging SFAC for Downstream Bandwidth

Cisco IOS Release 12.3(21)BC supports the debugging of downstream bandwidth resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Setting Downstream and Upstream Application Thresholds, on page 1522

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control ds-bandwidth** **Example:** `Router# debug cable admission-control ds-bandwidth`	Enables downstream throughput troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control ds-bandwidth** command.

```
Router# debug cable admission-control ds-bandwidth
Oct  8 23:29:11: Failed to allocate DS bandwidth for
CM 0007.0e01.1db5 in adding a new service entry
```

Debugging SFAC for Upstream Throughput

Cisco IOS Release 12.3(21)BC supports the debugging of upstream bandwidth resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Setting Downstream and Upstream Application Thresholds, on page 1522

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control us-bandwidth** **Example:** `Router# debug cable admission-control us-bandwidth`	Enables enable upstream throughput troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control us-bandwidth** command.

```
Router# debug cable admission-control us-bandwidth
Router#
Oct  8 23:29:11: Failed to allocate US bandwidth for
CM 0007.0e01.9b45 in adding a new service entry
```

Debugging Flow Categorization for SFAC

Cisco IOS Release 12.3(21)BC introduces a new **debug** command that accounts for the bucket-flow scheme of SFAC. This **debug** command displays service flow categorization results—when a service flow is classified, the **debug** command displays the application by which it was categorized, along with which rule is matched.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Defining Rules for Service Flow Categorization, on page 1518

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control flow-categorization** **Example:** `Router# debug cable admission-control flow-categorization`	Enables debugging of service flow categorization processes for SFAC. This command displays service flow categorizations currently enabled on the Cisco CMTS. Use the **no** form of this command to disable this debugging.

Below is a shortened example of the information displayed when the **debug cable admission-control flow-categorization** command is enabled on the Cisco CMTS. This command displays interface-level information.

```
Router# debug cable admission-control flow-categorization
int ca 5/1/1 sfid 55 identified as video pcmm priority 6 matched.
```

Debugging Wideband Interfaces for SFAC

Cisco IOS Release 12.2(33)SCC supports debugging of the wideband interface for SFAC on the Cisco CMTS using a new **debug** command.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Defining Rules for Service Flow Categorization, on page 1518

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**debug cable wbcmts admission-control** **Example:** `Router# debug cable wbcmts admission-control`	Enables debugging of the wideband interface admission control on the Cisco CMTS. Use the **no** form of this command to disable this debugging.

The following example shows a sample output of the **debug cable wbcmts admission-control** command.

```
Router> enable
Router# debug cable wbcmts admission-control
Oct  5 15:43:32.230: Wideband-Cable1/0/0:0    NB 6/1/0 app 1, nb cir = 0, total bkt cir =
0
Oct  5 15:43:32.230:  total_cfg_non_ex_pct: 0, prev_bkt_resv: 0
Oct  5 15:43:32.230: total_cfg_ex_pct: 100, total_cfg_non_ex_pct: 0, total_ex_cir_cfg_bps:
 72000000, total bkt resv 0
Oct  5 15:43:32.230: Wideband-Cable1/0/0:0    app 1, per_bucket_cfg_excl_bps: 0,
max_non_ex_bps: 0,
total_nonex_resvd_bps: 0, bkt type: 0
```

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting SFAC on the Cisco CMTS:

- Displaying Application Buckets for SFAC, on page 1529
- Displaying Service Flow Reservation Levels, on page 1529
- Debugging SFAC for Different Event Types, on page 1532
- Debugging SFAC for CPU Resources, on page 1533
- Debugging SFAC for Memory Resources, on page 1533
- Debugging SFAC for Downstream Bandwidth, on page 1534
- Debugging SFAC for Upstream Throughput, on page 1535
- Debugging Flow Categorization for SFAC, on page 1535

Troubleshooting Tips

SFAC supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

If SFAC checks fail for memory resources, refer to the following sections for additional information about memory thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 1513

Configuration Examples for SFAC

This section describes solutions-level examples of the SFAC feature on the Cisco CMTS. This section illustrates the functioning of SFAC in default or non-default but properly operational configurations. This section presumes the proper use of configuration and monitoring procedures and commands described elsewhere in this document.

This section contains the following examples to illustrate SFAC:

Example: SFAC Configuration Commands

In this section of configuration examples, the following SFAC parameters are set on the Cisco CMTS:

- All the packetcable flows are mapped into bucket 1.
- The BE service flows are mapped into bucket 8.

The following configuration commands enable these settings:

- To map the packetcable voice flows, these commands are used:

```
cable application-type 1 include packetcable normal
cable application-type 1 include packetcable priority
cable application-type 1 name PktCable
```

- To map the BE flows into bucket 8, these commands are used.

```
cable application-type 8 name HSD
cable application-type 8 include best-effort
```

- Given the above configurations, you may also control bandwidth allocation to a PCMM streaming video application. The streaming video application is identified by the PCMM application ID 35. The following commands implement this configuration:

```
cable application-type 2 name PCMM-Vid
cable application-type 2 include pcmm app-id 35
```

- These configurations may be verified on the Cisco CMTS using the following **show** commands:

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

These above configuration examples might be omitted or changed, but the remaining examples in this section presume the above configurations.

Example: SFAC for Downstream Traffic

This example presumes that you have configured the rules according to the commands illustrated at the start of this section. All the voice flows in bucket 1. All the CIR data flows are categorized in bucket 8.

This example illustrates a sample configuration for SFAC with downstream traffic. In this example, if voice traffic exceeds 30% bandwidth consumption, additional voice flows are denied.

- 30% downstream throughput is reserved exclusively for voice traffic.
- Minor and major alarms for voice traffic to be generated at 15% and 25% respectively.

The following Cisco IOS command implements this configuration:

```
Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25 exclusive
 30
```

In this example, the voice flows are rejected when the bandwidth usage of the flows exceeds 30%.

In addition, you can allow for some flexibility by allowing flows to exceed their exclusive share, and to consume up to 50% of the total downstream throughput (30% + 20%). The following command accomplishes this:

```
Router(config)# cable admission control downstream bucket-no 1 minor 15 major 25 exclusive
 30 non-exclusive 20
```

With this previous command, the bucket 1 flows are rejected when the voice usage exceeds 50% (30% + 20%).

Similarly you can configure data thresholds as follows:

```
Router(config)# cable admission control bucket-no 8 minor 15 major 25 exclusive 50
non-exclusive 10
```

With the configuration commands as above, the following multi-stage scenario illustrates how the lending and borrowing of throughput is achieved in the presence of multiple traffic classes.

Stage I—Initial Throughput Allocations

Assume downstream throughput distribution is as follows:

- Downstream voice threshold is configured at 30%, with current consumption at 20%.
- Downstream data threshold is configured at 50%, with current consumption at 40%.

Table below summarizes this throughput distribution:

Table 163: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Bucket-no 1 (Voice)	30%	20%	20%	30%
Bucket-no 8 (Data)	50%	10%	40%	20%
Uncategorized Traffic			0%	40% (100% -20% - 40%)

Stage 2—Voice Traffic Exceeds 30% Exclusive Throughput

Now assume conditions change as follows:

- Voice throughput increases to 40%. Voice obtains 10% from the non-exclusive share.
- Data (Best Effort CIR) throughput usage increases to 50%, consuming all exclusive data throughput.
- Bandwidth available for uncategorized traffic shrinks to 30%.

Table below summarizes this throughput distribution:

Table 164: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	10%
Data	50%	10%	50%	10%
Uncategorized Traffic			0%	10% (100% - 40% - 50%)

Step 3—Bandwidth Consumption Increases by 10%

Now assume that data throughput usage increases by 10% for a new consumption total of 60%, and voice usage remains same. This consumes all remaining non-exclusive bandwidth from Best Effort.

Table below summarizes this throughput distribution:

Table 165: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	0%
Data	50%	10%	60% (50% + 10%)	0%
Uncategorized Traffic				0% (100%-40%-60%)

Note For the first time in this multi-stage example, bandwidth consumption on the Cisco CMTS has reached 100%, and there is no bandwidth available for uncategorized flows after the events of Stage 3.

Example: SFAC for Bonding Groups

This example shows configuration of SFAC with the following line card configurations:

- Modular cable interface with 3 Gigabit Ethernet cards
- Wideband interface with 3 Gigabit Ethernet cards
- MC20x20 line card with 3Gigabit Ethernet cards

```
Router(config-if)#cable application-type 1 include scheduling-type ugs
Router(config-if)#cable application-type 1 include packetcable normal
Router(config-if)#cable application-type 1 include packetcable high-priority
Router(config-if)#cable application-type 1 include pcmm priority 2
Router(config-if)#cable application-type 2 include BE
Router(config-if)#cable application-type 3 include multicast 12
!
Router(config)#interface Wideband-Cable1/0/0:0
 cable bundle 2
 cable bonding-group-id 1
 cable rf-channel 1
 cable rf-channel 2
 cable rf-channel 3 bandwidth-percent 1
Router(config-if)#cable admission-control max-reserved-bandwidth 60302
Router(config-if)#cable admission-control ds-bandwidth 1 minor 10 major 20 exclusive 30
non-exclusive 40
Router(config-if)#cable admission-control ds-bandwidth 2 minor 5 major 10 exclusive 15
non-exclusive 25
```

Additional References

The following topics provide references related to SFAC for the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS Cable Commands	Cisco CMTS Cable Command Reference
DOCSIS 1.1 for the Cisco CMTS Routers	*DOCSIS 1.1 for the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis11.html
CISCO-CABLE-ADMISSION-CTRL-MIB for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Series Router MIB Specifications Guide 12.2 SC* http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html

Standards

Standard	Title
CableLabs™ DOCSIS 1.1 specifications	http://www.cablelabs.com/cablemodem/

Standard	Title
CableLabs™ PacketCable specifications	http://www.cablelabs.com/packetcable/
CableLabs™ PacketCable MultiMedia specifications	http://www.cablelabs.com/packetcable/specifications/multimedia.html

MIBs

MIB	MIBs Link
MIBs for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Series Router MIB Specifications Guide 12.2 SC* http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html
MIBs Supporting Cisco IOS	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SFAC for the Cisco Cable Modem Termination System

Table below lists the release history for this feature.

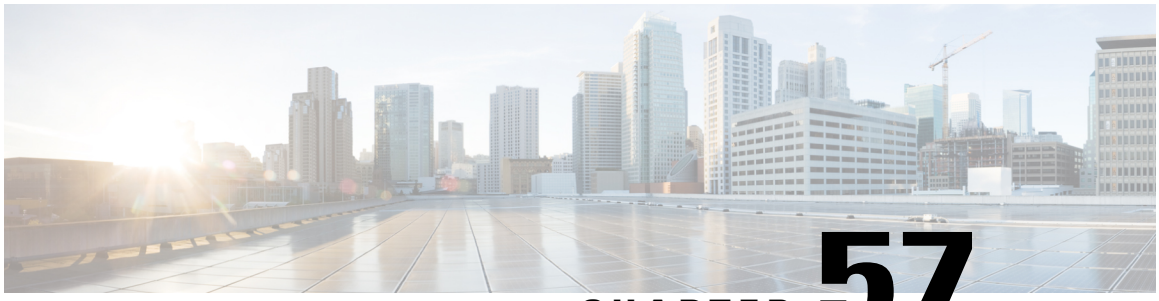
Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on Cisco.com is not required.

Note Table 166: Feature Information for Admission Control , on page 1543 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 166: Feature Information for Admission Control

Feature Name	Releases	Feature Information
Admission Control for the Cisco CMTS Routers	12.3(13a)BC	The Service Flow Admission Control feature was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers.
Service Flow Admission Control for the Cisco CMTS Routers	12.3(21)BC	This feature was introduced on the Cisco uBR10012 and the Cisco uBR7246VXR universal broadband routers. It supersedes the previous form of admission control supported on these CMTSs.
Service Flow Admission Control for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.
Service Flow Admission Control for Bonding Groups.	12.2(33)SCC	The Service Flow Admission Control feature has been updated to extend the functionality to US and DS bonding groups to Cisco uBR10012 routers.
Service Flow Admission Control for Bonding Groups.	12.2(33)SCD	The Service Flow Admission Control feature has been updated to extend the functionality to US and DS bonding groups for Cisco uBR7200 series routers.



CHAPTER 57

Subscriber Traffic Management for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This document contains information that references many legacy documents from Cisco IOS Release 12.3BC. In general, references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC. The updates to this feature in Cisco IOS Release 12.3(23)BC2 are supported from Cisco IOS Release 12.2(33)SCB and later.

This document describes the Subscriber Traffic Management (STM) feature Version 1.3. STM feature supports all DOCSIS-compliant cable modems.

The STM feature allows a service provider to configure a maximum bandwidth threshold over a fixed period for a specific service class (or quality of service [QoS] profile)). The subscribers who exceed this configured threshold can then be identified and allocated reduced QoS. STM works as a low-CPU alternative to Network-Based Application Recognition (NBAR) and access control lists (ACLs). However, using STM does not mean that NBAR and ACLs have to be turned off; STM can be applied along with NBAR and ACLs. STM also works in conjunction with the Cisco Broadband Troubleshooter to support additional network management and troubleshooting functions in the Cisco CMTS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Subscriber Traffic Management on the Cisco CMTS Routers

The Subscriber Traffic Management feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 167: Cable Hardware Compatibility Matrix for the Subscriber Traffic Management feature

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later releases** • Cisco uBR-MC3GX60V [108]
Cisco uBR7246VXR Universal Broadband Routers	**Cisco IOS Release 12.3(21)BC and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2)	**Cisco IOS Release 12.3(21)BC and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [109]

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC28U/X • Cisco uBR-MC88V

108 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

109 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Subscriber Traffic Management on the Cisco CMTS Routers

Note In this document, the phrase QoS profile is synonymously used to indicate a service class for a DOCSIS 1.1 cable modem. However, QoS profile applies only to DOCSIS 1.0 operations. In instances where QoS profile is mentioned to indicate DOCSIS 1.1 operations, the QoS profile should be treated as a service class.

The STM feature has the following restrictions and limitations:

- Cisco IOS Release 12.2(15)BC1 supports monitoring and controlling only cable modems that have registered for DOCSIS 1.0 operations (using the quality of service [QoS] profile or service ID [SID] model).
- Cisco IOS Release 12.3(9a)BC supports monitoring and controlling cable modems that have registered for DOCSIS1.0 or DOCSIS 1.1 operations (using the QoS profile ID or service ID [SID] model).
- In STM version 1.1, the sampling rate range (duration) is calculated using the monitoring duration rather than the constant range (10 to 30 minutes) used in STM 1.0.
  - If the monitoring duration is more than a day (1440 minutes), the duration sample rate is calculated as (duration / 100).
  - If the monitoring duration is less than a day, the sample rate range is from 10 to 30 minutes.
  - If you are using STM 1.0 with a duration of two days and a sample rate of 20 minutes, and you try to restore that configuration in STM 1.1, the command fails because now the valid range is from 28 to 86 minutes.
- For DOCSIS1.0, the registered QoS profile specified by an enforce-rule must match exactly a QoS profile that exists on the Cisco CMTS. To manage a cable modem that is using a modem-created QoS profile, you must first create that same exact QoS profile on the Cisco CMTS. All parameters in the QoS profile must match before the cable modem can be managed by the enforce-rule.
- The Cisco CMTS routers support a certain maximum number of enforce-rules depending on your Cisco IOS software release. If you have created the maximum number of enforce-rules and want to create another rule, you must first delete one of the existing rules.

  - Cisco IOS Release 12.2(15)BC1 and later—Supports a maximum of 20 enforce-rules.
  - Beginning in Cisco IOS Release 12.3(23)BC2—Supports a maximum of 40 enforce-rules.

- Changing the configuration of an enforce-rule automatically resets all byte counters for the subscribers who are mapped to that enforce-rule.
- When specifying a QoS profile to be enforced when users violate their registered QoS profiles, both the originally provisioned QoS profile and the enforced QoS profile must be created on the Cisco CMTS.
- The Subscriber Traffic Management feature calculates duration based on the time set on the router, not uptime. Therefore, if you use the **clock set** command to change the time on the router, you might affect the STM monitoring behavior.
- The maximum cycle for subscriber traffic management is 31 days. If you choose a cycle of 31 days, the minimum sample rate that you can set is (31 days/100) minutes.

Information About Subscriber Traffic Management on the Cisco CMTS Routers

This section contains the following:

Feature Overview

The STM feature allows service providers to configure a maximum bandwidth threshold over a fixed period, for a specific service class (or QoS profile). The subscribers who exceed this configured threshold can then be identified and allocated a reduced QoS. This feature supplements current techniques such as NBAR and ACLs, to ensure that a minority of users do not consume a majority of a cable network's bandwidth.

Current subscriber controls, such as NBAR and ACLs, examine all packets coming into the CMTS. These techniques can curb a large volume of problem traffic, but they are not as effective in dealing with the latest generation of peer-to-peer file-sharing applications that can place heavy demands on a network's available bandwidth.

The STM feature allows service providers to focus on a minority of potential problem users without impacting network performance or other users who are abiding by their service agreements.

The STM feature supports two types of monitoring:

- Legacy Monitoring—Legacy monitoring allows you to set up a single monitoring duration without the ability to choose the time of day when that monitoring is performed. The configured monitoring parameters remain constant throughout the day.
- Peak-Offpeak Monitoring—Peak-Offpeak monitoring allows you to specify up to two high-traffic periods in a day for monitoring, in addition to the ability to continue monitoring during the remaining (or off-peak) periods. By combining the peak time option with weekend monitoring, you can identify and limit the bandwidth usage of certain subscribers for up to two peak network usage periods during weekdays, and during a different set of peak usage periods on weekends.

When a cable modem goes offline and remains offline for 24 hours, the Cisco CMTS router deletes its service flow IDs from its internal databases, and also deletes the modem's traffic counters. This can allow some users to exceed their bandwidth limits, go offline, and come back online with new counters. The Subscriber Traffic Management feature helps to thwart these types of theft-of-service attacks by implementing a penalty period

for cable modems that violate their service level agreements (SLAs). Even if a cable modem goes offline, its counters are still reset, and the CMTS continues to enforce the penalty period.

Feature List

The Subscriber Traffic Management feature has the following operational features:

- Subscriber Traffic Management 1.1 (STM 1.1) supports cable modems that have registered for DOCSIS 1.1 operations (using the service class/service flow ID [SFID] model).
- Up to 20 enforce-rules can be created on each CMTS in Cisco IOS software releases prior to Cisco IOS Release 12.3(23)BC2. Beginning in Cisco IOS Release 12.3(23)BC2, you can create up to 40 enforce-rules.
- Separate enforce-rules can be used for downstream traffic and for upstream traffic. However, the limit on the total number of enforce-rules that can be configured includes the upstream and downstream rules combined.
- Each enforce-rule uses a subscriber's registered QoS profile to identify which users should be monitored for excessive traffic. The registered QoS profile must exist on the Cisco CMTS. If you want to manage cable modems that are using QoS profiles that were created by the cable modem, you must first manually create a QoS profile with the exact same QoS parameters on the Cisco CMTS, and then allow the cable modem to come online using the manually created profile.
- Each enforce-rule specifies the maximum number of kilobytes a user can transmit during a specified window.
- Subscribers who exceed the maximum bandwidth that is specified by their enforce-rule can be automatically switched to a separate enforced QoS profile that limits their network use for a customizable penalty period. The enforced QoS profile can change the guaranteed bandwidth, priority, or any other aspect of the traffic that the service provider considers an acceptable response to subscribers who violate their service agreements.
- Subscribers are automatically switched back to their registered QoS profile at the end of their penalty period. A technician at the service provider's network operations center (NOC) can also switch them back before the penalty period expires.

  Note To manually switch back, delete the cable modem and allow it to register again.

- This feature also supports a **no-persistence** option, so that the enforced QoS profile does not remain in effect when a cable modem reboots. This option is particularly useful when the feature is initially implemented, so that the service providers can identify problem subscribers and applications, without creating a major impact on the entire user base. When repeat offenders are found, they can then be switched to an enforce-rule that does keep the enforced QoS profile in effect even when the cable modem reboots.
- Service providers can display a list of all subscribers' current usage statistics. Service providers can also display a list of just those subscribers who are overconsuming bandwidth.
- The penalty period persists across reboots of the cable modem, so subscribers cannot avoid the enforced QoS profile by resetting their modems and reregistering on the cable network. This allows service providers to set an appropriate penalty for those users that consistently exceed the maximum bandwidth

they have been allocated. Service providers also can specify a time of day when CMs that are identified for penalty can be released from the penalty period.

- If a user that is using excessive bandwidth decides to upgrade to a higher level of service, the service provider can reconfigure the provisioning system to assign a new QoS profile to the cable modem. The user can then reboot the cable modem and come online using the new level of service.
- Service providers can change subscriber service classes for a particular modem using the **cable modem service-class-name** command.
- Different subscriber monitoring parameters can be configured for weekends, including peak and offpeak monitoring windows. You can also establish the same monitoring windows for every day of the week, or turn off monitoring altogether on the weekends as desired.

Sliding Window for Monitoring Service Flows

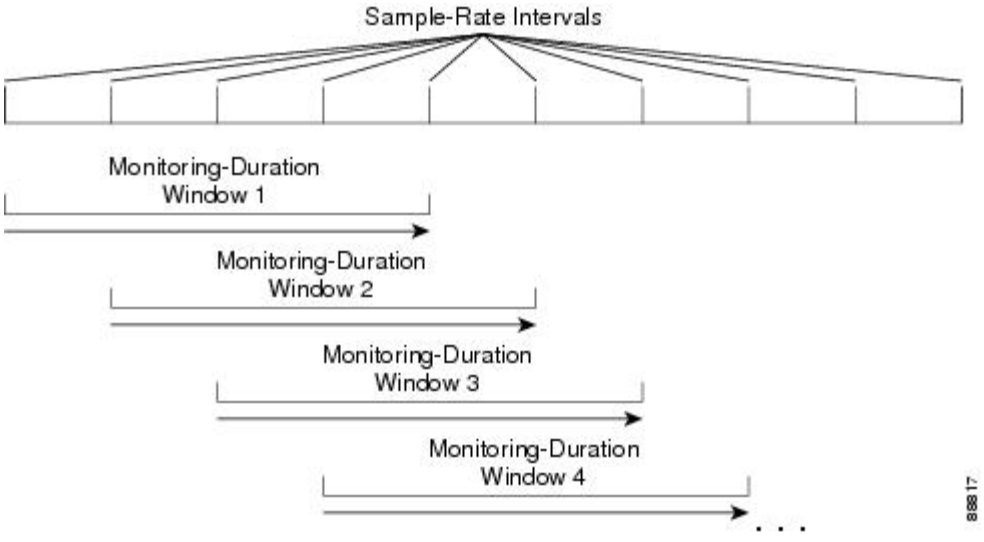
When an enforce-rule is activated, the CMTS periodically checks the bandwidth being used by subscribers to determine whether any subscribers are consuming more bandwidth than that specified by their registered QoS profiles. The CMTS keeps track of the subscribers using a sliding window that begins at each sample-rate interval and continues for the monitoring-duration period.

Each sample-rate interval begins a new sliding window period for which the CMTS keeps track of the total bytes transmitted. At the end of each sliding window period, the CMTS examines the byte counters to determine if any subscriber is currently overconsuming bandwidth on the network.

For example, with the default sample-rate interval of 15 minutes and the default monitoring-duration window of 360 minutes (6 hours), the CMTS samples the bandwidth usage every 15 minutes and determines the total bytes transmitted at the end of each 360-minute window. Therefore, every 15 minutes, the CMTS determines each subscriber's usage statistics for the preceding 6-hour period.

Figure below illustrates how this process works, with a new sliding window beginning at the beginning of each sample-rate interval period.

Figure 32: Monitoring-Duration Windows



Weekend Monitoring

With standard legacy and peak-offpeak monitoring configuration, monitoring continues to occur on the weekends, but in releases prior to Cisco IOS Release 12.3(23)BC2, there was not an ability to establish different monitoring criteria during the weekend days.

Beginning in Cisco IOS Release 12.3(23)BC2 for STM version 1.2, support for configuration of different monitoring conditions on weekends is introduced. Weekend monitoring options support the same parameters that are available in the existing monitoring options, but use a separate set of commands to configure alternate monitoring on weekend days. This includes configuration of peak and offpeak weekend monitoring windows.

In addition, the CLI supports the ability to turn off any monitoring on the weekend, or to use the same monitoring conditions for every day of the week.

SNMP Trap Notifications

Cisco IOS Release 12.2(15)BC1 (for the Cisco uBR10012 router) and Cisco IOS Release 12.3(9a)BC (for the Cisco uBR7246VXR router and the Cisco uBR7100 series routers) support a Simple Network Management Protocol (SNMP) trap notification that can be sent whenever a subscriber violates the enforce-rule. This trap is defined in the CISCO-CABLE-QOS-MONITOR-MIB and is enabled using the **snmp-server enable traps cable** command.

Each SNMP trap notification contains the following information:

- MAC address of the subscriber's cable modem
- Name of the enforce-rule being applied to this subscriber
- Total bytes sent by the subscriber during the monitoring-duration window
- Time at which the subscriber's penalty period expires

The CISCO-CABLE-QOS-MONITOR-MIB also contains the following tables that provide information about the Subscriber Traffic Management configuration and about subscribers who violate their enforce-rules:

- ccqmCmtsEnforceRuleTable—Contains the attributes of the enforce-rules that are currently configured on the Cisco CMTS.
- ccqmEnfRuleViolateTable—Provides a snapshot list of the subscribers who violated their enforce-rules over the sliding monitoring-duration window.

Beginning in Cisco IOS Release 12.3(23)BC2, the following new objects are introduced to support feature enhancements in STM Version 1.2:

- ccqmCmtsEnfRulePenaltyEndTime
- ccqmCmtsEnfRuleWkndOff
- ccqmCmtsEnfRuleWkndMonDuration
- ccqmCmtsEnfRuleWkndAvgRate
- ccqmCmtsEnfRuleWkndSampleRate
- ccqmCmtsEnfRuleWkndFirstPeakTime
- ccqmCmtsEnfRuleWkndFirstDuration

- ccqmCmtsEnfRuleWkndFirstAvgRate
- ccqmCmtsEnfRuleWkndSecondPeakTime
- ccqmCmtsEnfRuleWkndSecondDuration
- ccqmCmtsEnfRuleWkndSecondAvgRate
- ccqmCmtsEnfRuleWkndOffPeakDuration
- ccqmCmtsEnfRuleWkndOffPeakAvgRate
- ccqmCmtsEnfRuleWkndAutoEnforce

Beginning in Cisco IOS Release 12.3(33)SCD2, the following new objects are introduced to support feature enhancements in STM Version 1.3:

- ccqmCmtsEnfRuleFirstPeakTimeMin
- ccqmCmtsEnfRuleSecondPeakTimeMin
- ccqmCmtsEnfRuleWkndFirstPeakTimeMin
- ccqmCmtsEnfRuleWkndSecondPeakTimeMin
- ccqmCmtsEnfRulePenaltyEndTimeMin
- ccqmCmtsEnfRuleWkPenaltyPeriod
- ccqmCmtsEnfRuleWkndPenaltyPeriod
- ccqmCmtsEnfRuleRelTimeMonitorOn

Restrictions for SNMP Trap Notifications

In Cisco IOS Release 12.3(23)BC2, the MIB objects for weekend monitoring support only the SNMP GET and GETMANY operations.

Cable Modem Interaction with the Subscriber Traffic Management Feature

The Subscriber Traffic Management feature ensures that users cannot bypass the QoS restrictions by rebooting their cable modems or performing other configuration changes. The service provider, however, continues to be able to change the modems' profiles and other configuration parameters as desired.

When the Subscriber Traffic Management feature is enabled, the following behavior is in effect:

- The primary service flow counters for downstream and upstream traffic are preserved when the cable modem reboots. The service provider, however, can reset the counters by changing the QoS profile for the cable modem using the **cable modem qos profile** command and resetting the cable modem.
- Secondary service flow counters are reset whenever the cable modem reboots. This happens regardless of the enforce-rule configuration.
- The cable modem retains its current primary downstream and upstream service flows when it reboots. If the cable modem is in an enforced QoS profile penalty period when it reboots, it continues using the enforced QoS profile after the reboot. Service providers can manually change the profile by assigning a new QoS profile using the **cable modem qos profile** command.

Note Changing the QoS profile for a cable modem using the **cable modem qos profile** command, also changes the enforce-rule for the cable modem when it reboots. When the cable modem comes back online, it begins operating under the enforce-rule whose registered QoS profile (see the **qos-profile registered** command) matches the new QoS profile the modem is using.

- Service providers can also change the enforce-rule configuration. The following happens when the provider changes the enforce-rule configuration:
  - If the enforce-rule is disabled (using the **no enabled** command), all cable modems using that rule's registered QoS profile are no longer managed by the Subscriber Traffic Management feature. Configuring no enabled, deactivates the enforce-rule and moves all the modems in penalty to its registered QoS.
  - If the registered QoS profile for the rule is changed (using the **qos-profile registered** command), the cable modems that are using the previous registered QoS profile are no longer managed by the Subscriber Traffic Management feature. Instead, any cable modems that use the new registered QoS profile begin being managed by this rule.
  - If the enforced QoS profile for the rule is changed (using the **qos-profile enforced** command), any cable modems using this rule that are currently in the penalty period continue using the previously configured enforced QoS profile. Any cable modems that enter the penalty period after this configuration change, however, use the new enforced QoS profile.
- Service providers also have the option of making an enforce-rule nonpersistent, so that the enforced QoS profile does not remain in force when a cable modem reboots. Instead, when the cable modem reboots and reregisters with the Cisco CMTS, the CMTS assigns it the QoS profile that is specified in its DOCSIS configuration file.

How to Configure the Subscriber Traffic Management Feature on the Cisco CMTS Routers

This section contains the following:

Creating and Configuring an Enforce-Rule

Every service class name that needs to be monitored will be linked with an enforce-rule. An enforce-rule defines the monitoring duration, the sample rate, the penalty period, and the registered service class name that the enforce-rule is linked to and the enforced service class name.

Use the procedure given below to create and configure an enforce-rule. An enforce-rule does not become active until the **enabled** command is given.

Before You Begin

- The registered and enforced service (QoS) profiles must be created on the CMTS before creating an enforce-rule that uses those profiles. If you want to manage a cable modem that currently uses a modem-created QoS profile, you must first manually create a new QoS profile on the CMTS with the same QoS parameters as the modem-created profile. Then allow the modem to come online using the manually created profile before beginning this procedure.

- To display quality of service (QoS) profiles for a Cisco CMTS, use the show cable qos profile command in privileged EXEC mode.
- To configure a QoS profile, use the cable qos profile command in global configuration mode. To set a particular value to its default, or to delete the profile when no specific parameters have been set, use the no form of this command.

- For monitoring of DOCSIS 1.1 cable modems:
  - Only DOCSIS 1.1 modems that register with a service class name are monitored.
  - To ensure that the DOCSIS 1.1 service flow counters remain across a reboot of the CM, configure the **cable primary-sflow-qos11 keep all** global configuration command.
- Only primary upstream and downstream service flows are supported.

Restriction

- When configuring peak-offpeak monitoring, you can define a maximum of two peak durations within a day, and also monitoring of the remaining hours, if you configure the offpeak duration. The monitoring duration and threshold for first peak, second peak, and offpeak, can be different. However, the monitoring duration for any peak or offpeak configuration cannot be more than a day.
- The parameters defined by the named service class should always be a compatible subset of the registered set of parameters for the CM. Only certain options can be changed using a CMTS router service class, such as the **max-rate**, **priority**, or **tos-overwrite** options. The **max-burst** option in both the enforced and registered CMTS router service classes must strictly match the value for **max-burst** in the registered DOCSIS configuration file. If the service class value does not match, either the cable modem registration will fail with a reject-c state, or the enforced class will fail.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Creates an enforce-rule with the specified *name* and enters the enforce-rule configuration mode. The *name* parameter can be any arbitrary and unique string that is from 1 to 15 characters in length. **Note** Each enforce-rule can be created by giving it a name.

	Command or Action	Purpose
Step 4	**monitoring-basics** {**legacy** | **peak-offpeak**} {**docsis10** | **docsis11**} **Example:** `Router(enforce-rule)# monitoring-basics peak-offpeak docsis11`	Defines the kind of monitoring desired and the type of modems to be monitored. • **legacy—**Provides only one threshold and one monitoring duration. • **peak-offpeak—**Allows the selection of two peak durations within a day. • **docsis10—**Specifies application of the enforce-rule to DOCSIS 1.0 cable modems. • **docsis11—**Specifies application of the enforce-rule to DOCSIS 1.1 cable modems. The default is legacy and DOCSIS 1.0.
Step 5	**qos-profile registered** *profile-id* **Example:** `Router(enforce-rule)# qos-profile registered 1`	Specifies the registered quality of service (QoS) profile that should be used for this enforce-rule. *profile-id* is a number from 0 to 16383. **Note** If you want to manage a cable modem that currently uses a modem-created QoS profile, you must first manually create a new QoS profile on the CMTS with the same QoS parameters as the modem-created profile. Then allow the modem to come online using the manually created profile before using this command.
Step 6	**qos-profile enforced** *profile-id* [**no-persistence**] **Example:** `Router(enforce-rule)# qos-profile enforced 4`	Specifies the quality of service (QoS) profile that should be enforced when users violate their registered QoS profiles. • *profile-id* Number from 0 to 16383. • **no-persistence—**(Optional) Configures the rule so that the enforced QoS profile does not remain in effect when a cable modem reboots.
Step 7	**service-class** {**enforced** | **registered**} *name* **Example:** `Router(enforce-rule)# service-class enforced test`	Identifies a particular service class with the specified *name* for cable modem monitoring in an enforce-rule. • **enforced—**Specifies an enforced service class. • **registered—**Specifies the service class using which the cable modem registered. **Note** This command is applicable only for DOCSIS 1.1 (or later) cable modems.
Step 8	**duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**} [**enforce**] **Example:** `Router(enforce-rule)# duration 10 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	Specifies the time period and sample rate used for monitoring subscribers when legacy monitoring is configured (Step 4, on page 1555). • *minutes*—Specifies the size of the sliding window (in minutes) during which subscriber usage is monitored. The valid range is 10 to 44640, with a default of 360 (6 hours). • **avg-rate** *rate*—Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 with no default.

	Command or Action	Purpose
		• **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate o f subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes. • **penalty**—(Optional) Specifies the period (in minutes) during which a cable modem can be under penalty. This weekday penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080. • **downstream**—Specifies monitoring of traffic in the downstream direction. • **upstream**—Specifies monitoring of traffic in the upstream direction. • **enforce**—(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.
Step 9	**peak-time1** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate*][**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**}[**enforce**] **Example:** `Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce` `Router(enforce-rule)# peak-time1 6:30 duration 180 avg-rate 2 peak-time2 18:40 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`	Specifies peak monitoring periods when peak-offpeak monitoring is configured (Step 4, on page 1555). • **peak-time1** {*hour* | *hour:minutes*}—Specifies the time of day during which monitoring occurs for the first peak time. This value can be specified in hour (hh) or hour:minutes (hh:mm) format. The valid range for hour is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59. • **duration** *minutes*—Specifies the size of the sliding window during which the subscriber usage is monitored for the first peak time, and optionally for a second peak time when used with the **peak-time2** keyword. Valid range is 60 to 1440 minutes. • **avg-rate** *rate*—Specifies the average sampling rate in kilobytes per second for the specified duration. The valid range is 1 to 400000 with no default. • **peak-time2** {*hour* | *hour:minutes*}—(Optional) Specifies the time of day during which monitoring occurs for a second peak time. This value can be specified in hour (hh) or hour:minutes (hh:mm) format. The valid range for hours is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59. • **duration** *offpeak-minutes*—(Optional) Specifies the size of the sliding window during which the subscriber usage is monitored for the remaining offpeak time (time not specified for peak monitoring). The valid range is 60 to 1440 minutes. • **avg-rate** *offpeak-rate*—(Optional) Specifies the average sampling rate in kilobytes per second for the specified offpeak duration. The valid range is 1 to 400000 with no default. • **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes. • **penalty**—(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekday penalty duration, if configured, takes

	Command or Action	Purpose
		precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080.
Step 10		• **downstream—**Specifies monitoring of traffic in the downstream direction. • **upstream—**Specifies monitoring of traffic in the upstream direction. • **enforce—**(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates the registered QoS profile.
Step 11	**penalty-period** *minutes* [**time-of-day** {*hour*|*hour*:*minutes*}] [**monitoring-on**] **Example:** `Router(enforce-rule)# penalty-period 10`	(Optional) Specifies the period for which an enforced QoS profile should be in effect for subscribers who violate their registered QoS profiles. • *minutes***—**Number from 1 to 10080 minutes, with a default value of 10080 minutes (7 days). • **time-of-day** {*hour* |*hour*:*minutes*}**—**(Optional) Specifies the time of day when a penalized cable modem can be released from its enforced profile. The time can be specified in the hh (hours) or hh:mm (hours:minutes) format. The valid range for hours is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59. • monitoring-on**—**(Optional) Specifies that the monitoring should be turned on after the cable modem is released from the penalty, that is, after time-of-day. If this keyword is not specified, by default, monitoring is turned off after the release time.
Step 12	**enabled** **Example:** `Router(enforce-rule)# enabled`	(Optional) Activates the enforce-rule and begins subscriber traffic management.
Step 13	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Examples

This section provides command-line interface (CLI) examples, including the help feature for some of the enforce-rule commands.

Example: Legacy Monitoring Configuration

The following example shows a sample configuration of an enforce-rule for legacy monitoring:

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics ?
```

```
  legacy        Enable legacy (same average rate for all day)  monitoring
  peak-offpeak  Enable peak-offpeak monitoring
Router(enforce-rule)# monitoring-basics legacy ?
  docsis10  Enforce-rule will map to docsis 1.0 modems
  docsis11  Enforce-rule will map to docsis 1.1 modems
Router(enforce-rule)# monitoring-basics legacy docsis11
Router(enforce-rule)# service-class ?
  enforced    Enforced service class
  registered  Registered service class
Router(enforce-rule)# service-class registered ?
  WORD  Registered service class name
Router(enforce-rule)# service-class registered BEUS
Router(enforce-rule)# service-class enforced test
Router(enforce-rule)# duration ?
  <10-10080>  Duration in minutes
Router(enforce-rule)# duration 10 ?
  avg-rate  Average rate for the duration in kbits/sec
Router(enforce-rule)# duration 10 avg-rate ?
  <1-4294967>  average rate in kbits/sec
Router(enforce-rule)# duration 10 avg-rate 2 ?
  sample-interval  Rate of sampling in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 ?
  downstream  downstream
  upstream    upstream
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream enf
Router(enforce-rule)# $ avg-rate 2 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

Example: Peak-offpeak Monitoring Configuration

The following example shows a sample configuration of an enforce-rule for peak-offpeak monitoring:

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics peak-offpeak
Router(enforce-rule)# monitoring-basics peak-offpeak docsis10
Router(enforce-rule)# qos-profile ?
  enforced    Enforced qos profile
  registered  QoS profile index
Router(enforce-rule)# qos-profile registered ?
  <1-255>  Registered QoS profile index
Router(enforce-rule)# qos-profile registered 5
Router(enforce-rule)# qos-profile enforced 4
Router(enforce-rule)# peak-time1 6 ?
  duration  First peak duration
Router(enforce-rule)# peak-time1 6 duration ?
  <60-1440>  Duration in minutes
Router(enforce-rule)# peak-time1 6 duration 180 ?
  avg-rate  First peak average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 ?
  duration         Off-peak duration
  peak-time2       Second peak time
  sample-interval  Rate of sampling in minutes

Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 ?
  <10-1440>  Start of second peak time
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 ?
  duration  Second peak duration
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration ?
  <10-1440>  Duration in minutes
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration 240 ?
  avg-rate  Second peak average rate in kbits/sec
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
```

```
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 ?
  duration         Off-peak duration
  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 d
Router(enforce-rule)# $-time2 18 duration 240 avg-rate 3 duration 120 ?
  avg-rate  Off-peak average rate in kbits/sec
Router(enforce-rule)# $duration 240 avg-rate 3 duration 120 avg-rate 1 ?

  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $40 avg-rate 3 duration 120 avg-rate 1 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 ?

  downstream  downstream
  upstream    upstream
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# $on 120 avg-rate 1 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

Example: CLI Help for peak-time Command

The following example shows output from the CLI help for the **peak-time** command:

```
Router(enforce-rule)# peak-time ?

<0-23> Start of first peak time, use 24 hour clock

Router(enforce-rule)# peak-time 1 ?

duration First peak duration

Router(enforce-rule)# peak-time 1 d ?

<60-1440> Duration in minutes

Router(enforce-rule)# peak-time 1 d 65 ?

First peak average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a ?

<1-400000> Average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 ?

duration Off-peak duration

peak-time2 Second peak time

sample-interval Rate of sampling in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d ?

<60-1440> Duration in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 ?

avg-rate Off-peak average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a ?

<1-400000> Average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 ?

sample-interval Rate of sampling in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s ?
```

```
<1-30> Sampling rate in Minutes
Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 ?
downstream downstream
upstream upstream
Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 d ?
enforce enforce the qos-profile automatically
<cr>
Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 d
```

Configuring Weekend Monitoring

This section describes the tasks required to configure weekend monitoring for STM on a Cisco CMTS router.

Prerequisites

You must first configure the weekday monitoring parameters for an enforce-rule before configuring weekend monitoring. See the Creating and Configuring an Enforce-Rule, on page 1553.

Restrictions

- Up to 40 total enforce-rules across both upstream and downstream configurations are supported.
- When using SNMP for weekend monitoring, only SNMP GET and GETMANY operations are supported.

Configuring Different Legacy Monitoring Conditions for Weekends

Use the following procedure if you want to establish different legacy monitoring conditions for subscribers for either upstream or downstream traffic on weekend days.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**weekend duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes* {**downstream** | **upstream**} [**penalty** *minutes*] [**enforce**] **Example:** `Router(enforce-rule)# weekend duration 15 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	Specifies the time period and sample rate used for monitoring subscribers on weekends. • *minutes*—Specifies the size of the sliding window during which subscriber usage is monitored. The valid range is 10 to 44640, with a default of 360 minutes. • **avg-rate** *rate*—Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 with no default. • **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30, with a default value of 15. • **penalty**—(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekend penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080. • **downstream**—Specifies monitoring of traffic in the downstream direction. • **upstream**—Specifies monitoring of traffic in the upstream direction. • **enforce**—(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Configuring Different Peak-Offpeak Monitoring Conditions for Weekends

Use the following procedure if you want to establish different peak and offpeak monitoring conditions for subscribers for either upstream or downstream traffic on weekend days.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**weekend peak-time1** {*hour* | *hour*:*minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** *hour* **duration** *minutes* **avg-rate** *rate*] [**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream**| **upstream**}[**enforce**] **Example:** `Router(enforce-rule)# weekend peak-time1 9 duration 180 avg-rate 2 peak-time2 16 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce` **Example:** `Router(enforce-rule)# weekend peak-time1 9:30 duration 180 avg-rate 2 peak-time2 16:58 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`	Specifies peak and offpeak monitoring times on weekends. • **peak-time1** {*hour* | *hour:minutes*}**—**Specifies the first peak time, in hour (hh) or hour:minutes (hh:mm) format. The valid range for hours is 0 to 23 and for minutes is 0 to 59. • **duration** *minutes***—**Specifies the size of the sliding window during which subscriber usage is monitored for the first peak time, and optionally for a second peak time when used with the **peak-time2** keyword. The valid range is 60 to 1440 minutes. • **avg-rate** *rate***—**Specifies the average sampling rate in kilobytes per second for the specified duration. The valid range is 1 to 400000 with no default. • **peak-time2** {*hour* | *hour:minutes*}**—**(Optional) Specifies the second peak time, in hour (hh) or hour:minutes (hh:mm) format. The valid range for hour is 0 to 23 and for minutes is 0 to 59. • **duration** *offpeak-minutes***—**(Optional) Specifies the size of the sliding window during which the subscriber usage is monitored for the remaining offpeak time (time not specified for peak monitoring). The valid range is 60 to 1440 minutes. • **avg-rate** *offpeak-rate***—**(Optional) Specifies the average sampling rate in kbps for the specified offpeak duration. The valid range is 1 to 400000. • **sample-interval** *minutes***—**Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes.

	Command or Action	Purpose
		• **penalty—**(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekend penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080. • **downstream—**Specifies monitoring of traffic in the downstream direction. • **upstream—**Specifies monitoring of traffic in the upstream direction. • **enforce—**(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a users violate their registered QoS profile.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Disabling Weekend Monitoring

Use the following procedure to turn off the weekend monitoring configuration and monitor on weekdays only.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**weekend off** **Example:** `Router(enforce-rule)#  weekend off`	Disables monitoring on weekends.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Removing Weekend Monitoring Conditions and Use the Same Monitoring Criteria Every Day

Use the following procedure to remove the specified weekend monitoring conditions and use the same monitoring criteria all week (including weekends).

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**no weekend** **Example:** `Router(enforce-rule)# no weekend`	Performs monitoring on the weekends using the same parameters for weekdays and weekends.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Disabling an Enforce-Rule

Use the following procedure to disable an enforce-rule. The enforce-rule remains in the CMTS configuration file, but any subscriber traffic management that uses this enforce-rule ends.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos enforce-rule***name* **Example:** `Router(config)# cable qos enforce-rule test`	Creates an enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**no enabled** **Example:** `Router(enforce-rule)# no enabled`	Disables the enforce-rule and ends subscriber traffic management for users with the rule's registered QoS profile. It moves all modems in penalty to its registered QoS.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Removing an Enforce-Rule

Use the following procedure to delete an enforce-rule and remove it from the CMTS configuration file. Any subscriber traffic management that uses this rule also ends.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no cable qos enforce-rule***name* **Example:** `Router(config)# no cable qos enforce-rule ef-rule`	Deletes the enforce-rule with the specified *name* . This enforce-rule and its configuration are removed from the CMTS configuration, and any subscriber traffic management that uses this rule ends.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Changing a Cable Modem Service Class

Use the following procedure to change a QoS service class for a particular DOCSIS 1.1 cable modem.

Restriction

- The command is supported only on DOCSIS 1.1 CM primary service flows.
- You can specify the **cable modem service-class-name** command only after the CM has been online for at least 200 seconds.
- The parameters defined by the named service class should always be a compatible subset of the registered set of parameters for the CM. Only certain options can be changed using a CMTS router service class, such as the **max-rate**, **priority**, or **tos-overwrite** options. The **max-burst** option in both the enforced and registered CMTS router service classes must strictly match the value for **max-burst** in the registered DOCSIS configuration file. If the service class value does not match, then CM registration will fail with a reject-c state, or the enforced class will fail.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**cable modem** {*ip-address* | *mac-address*} **service-class-name** *name* **Example:** `Router# cable modem aaaa.bbbb.cccc service-class-name test`	Changes a QoS service class for a particular cable modem. • *ip-address*—Specifies the IP address of the CM to be assigned the named service class. • *mac-address*—Specifies the MAC address of the CM to be assigned the named service class. • *name*—Specifies the name of the QoS service class.
Step 3	**end** **Example:** `Router# end`	Exits privileged EXEC mode.

Monitoring the Subscriber Traffic Management Feature on the Cisco CMTS Routers

This section describes the following tasks that can be used to monitor the Subscriber Traffic Management feature:

Displaying the Currently Defined Enforce-Rules

To display all enforce-rules that are currently defined on the Cisco CMTS router, or the definitions for a particular enforce-rule, use the **show cable qos enforce-rule** command in privileged EXEC mode.

For offpeak monitoring, use the **show cable qos enforce-rule** command to display the monitoring duration and average-rate values applicable for that time of day. If no monitoring is taking place, 0 is displayed.

The following example shows sample output from the **show cable qos enforce-rule** command for all configured enforce-rules:

```
Router# show cable qos enforce-rule
            Name              Dur  Dir byte-cnt Auto rate  penalty Reg Enf Ena Persist
                             (min)     (kbytes) enf  (min) (min)   QoS QoS
 residential                  10   us  5        act  1     10080   5   10  Yes Yes
 ef-q11d                      30   ds  150      act  1     20      11  99  Yes Yes
 ef-q11u                      30   us  60       act  1     20      11  99  Yes Yes
 ef-q21                       720  us  60       act  1     10      21  81  Yes Yes
 ef-q21d                      300  ds  150      act  1     10      21  81  Yes Yes
 ef-q22                       720  us  60       act  1     10      22  82  Yes Yes
```

```
ef-q22d                     300  ds  150      act  1     10      22  82  Yes No
ef-q23                      720  us  60       act  1     10      23  83  Yes Yes
ef-q23d                     300  ds  150      act  1     10      23  83  Yes Yes
ef-q24                      720  us  60       act  1     10      24  84  Yes Yes
ef-q24d                     300  ds  150      act  1     10      24  84  Yes Yes
ef-q25                      720  us  60       act  1     10      25  85  Yes Yes
ef-q25d                     300  ds  150      act  1     10      25  85  Yes Yes
ef-q26                      720  us  60       act  1     10      26  86  Yes Yes
ef-q26d                     300  ds  150      act  1     10      26  86  Yes Yes
ef-q27                      720  us  60       act  1     10      27  87  Yes Yes
ef-q27d                     300  ds  150      act  1     10      27  87  Yes Yes
ef-q28                      720  us  60       act  1     10      28  88  Yes Yes
ef-q28d                     300  ds  150      act  1     10      28  88  Yes No
ef-q5d                      300  ds  150      act  1     10      5   99  Yes Yes
ef-q5u                      720  us  600      act  1     10      5   99  Yes Yes
```

The following example shows sample output from the **show cable qos enforce-rule** command for a particular enforce-rule named “test”:

```
Router# show cable qos enforce-rule test
     Name         Type Dur  Dir Avg-rate Auto rate     Reg        Enf      En Per
                      (min)     kbits/s  enf  (min)
test             p-off 120   us 1        act  10     255         4         Y  Y
```

The following example shows the sample output from the **show cable qos enforce-rule verbose** command for an enforce-rule named “test”:

```
Router# show cable qos enforce-rule test verbose
Name                          : test
Version                       : docsis11
Monitoring Type               : peak-offpeak
Registered                    : REG-DS
Enforced                      : ENF-DS
Monitoring Duration           : 70 (in minutes)
Sample-rate                   : 10 (in minutes)
Average-rate                  : 3 kbits/sec
Direction                     : downstream
Auto Enforce                  : Yes
Current Penalty Duration      : 10 (in minutes)
Default Penalty Duration      : 10 (in minutes)
Penalty End-time              : 23:0 (time of day)
Rule Enabled                  : Yes
Persistence                   : Yes
Weekend                       : No
Penalty Off                   : No
Monitor Weekend               : Yes
Monitoring after RelTime      : Off
First Peak Time               : 10:0
Duration                      : 60 (in minutes)
First Average-rate            : 1 kbits/sec
Second Peak Time              : 19:0
Duration                      : 65 (in minutes)
Second Average-rate           : 2 kbits/sec
Offpeak Duration              : 70 (in minutes)
Offpeak Average-rate          : 3 kbits/sec
Auto Enforce                  : Yes
Sample Rate                   : 10
Penalty-Period for week-days  : 0
Weekend First Peak Time       : 11:0
Weekend Duration              : 75 (in minutes)
Weekend First Average-rate    : 4 kbits/sec
Weekend Second Peak Time      : 20:0
Weekend Duration              : 80 (in minutes)
Weekend Second Average-rate   : 5 kbits/sec
Weekend Offpeak Duration      : 85 (in minutes)
Weekend Offpeak Average-rate  : 6 kbits/sec
Weekend Auto Enforce          : Yes
Weekend Sample Rate           : 12
Penalty-Period for week-ends  : 0
router#sh clock
*17:30:50.259 UTC Mon Apr 19 2010
```

The following example shows sample output from the **show cable qos enforce-rule verbose** command for a particular enforce-rule named "test" that has specified peak-offpeak weekend monitoring options:

```
Router# show cable qos enforce-rule test verbose
Name : test
Version : docsis10
Monitoring Type : peak-offpeak
Registered : 255
Enforced : 4
Monitoring Duration : 120 (in minutes)
Sample-rate : 10 (in minutes)
Average-rate : 1 kbits/sec
Direction : upstream
Penalty Time : 10080 (in minutes)
Penalty End-time : 23 (time of day in hrs)
Rule Enabled : Yes
Persistence : Yes
Week-end : Yes
First Peak Time : 6
Duration : 180 (in minutes)
First Average-rate : 2 kbits/sec
Second Peak Time : 18
Duration : 240 (in minutes)
Second Averate-rate : 3 kbits/sec
Offpeak Duration : 120 (in minutes)
Offpeak Average-rate : 1 kbits/sec
Auto-enforce : active
Weekend First Peak Time : 8
Weekend First Duration : 120 (in minutes)
Weekend First Average-rate : 2 kbits/sec
Weekend Second Peak Time : 18
Weekend Second Duration : 180 (in minutes)
Weekend Second Average-rate : 5 kbits/sec
Weekend Offpeak Duration : 240 (in minutes)
Weekend Offpeak Average-rate : 4 kbits/sec
Weekend Auto-enforce : active
```

Displaying the Current Subscriber Usage

To display the usage for all subscribers on a cable interface, use the show cable subscriber-usage command in privileged EXEC mode without any options.

To display the usage for just those subscribers who are violating their registered quality of service (QoS) profiles, use the show cable subscriber-usage over-consume form of the command.

The following example shows sample output from the **show cable subscriber-usage** command for all users on the specified cable interface:

```
Router# show cable subscriber-usage cable 6/0/1
Sfid Mac Address   Enforce-rule Total-Kbyte    Last-detect    Last-penalty   Pen
                       Name        Count         time           time        Flag
3    0007.0e03.110d efrule-q5   121944817  Jan1  03:44:08  Jan1  03:54:08  Act
4    0007.0e03.110d efrule-q5d  1879076068 Jan1  03:35:05  Jan1  03:45:06  Act
5    0007.0e03.1431 efrule-q5   120052387  Jan1  03:44:18  Jan1  03:54:18  Act
6    0007.0e03.1431 efrule-q5d  1838493626 Jan1  03:34:55  Jan1  03:44:55  Act
7    0007.0e03.1445 efrule-q5   120919427  Jan1  03:44:08  Jan1  03:54:08  Act
8    0007.0e03.1445 efrule-q5d  1865955172 Jan1  03:35:06  Jan1  03:45:06  Act
9    0007.0e03.1225 efrule-q5   120200155  Jan1  03:44:18  Jan1  03:54:18  Act
10   0007.0e03.1225 efrule-q5d  1839681070 Jan1  03:34:55  Jan1  03:44:55   -
11   0007.0e03.0cb1 efrule-q5   122941643  Jan1  03:43:58  Jan1  03:53:58  Act
12   0007.0e03.0cb1 efrule-q5d  1889107176 Jan1  03:35:06  Jan1  03:45:06  Act
13   0007.0e03.1435 efrule-q5   119504795  Jan1  03:44:18  Jan1  03:54:18  Act
14   0007.0e03.1435 efrule-q5d  1835164034 Jan1  03:34:55  Jan1  03:44:55   -
```

By default, the display is sorted by the service flow ID (SFID). To sort the display by the subscriber byte count, with the largest byte counts listed first, use the **sort-byte-count** option. The following example shows sample output for **show cable subscriber-usage sort-byte-count** form of the command:

Note The **sort-byte-count** option was replaced by the **sort-avg-rate** option.

```
Router# show cable subscriber-usage
 sort-byte-count

Sfid Mac Address   Enforce-rule Total-Kbyte  Last-detect    Last-penalty   Pen
                      Name        Count       time             time        Flag
7    0007.0e03.2cad test1       65157114   Feb24 11:36:34  Mar3  11:36:34  Act
9    0007.0e03.2c45 test1       16381014                                   -
5    0007.0e03.2c25 test1       13440960                                   -
```

Configuration Examples for Subscriber Traffic Management on the Cisco CMTS Routers

This section lists sample configurations for the Subscriber Traffic Management feature on a CMTS router:

Example: DOCSIS Configuration File and STM Service Classes

The following example shows a sample DOCSIS configuration file along with sample registered and enforced QoS service classes that you could define on a Cisco CMTS router to perform subscriber traffic management.

DOCSIS Configuration File Options

This is an example of a very basic set of options that you can configure for a cable modem in your DOCSIS configuration file that supports a successful configuration of new QoS service class options on the Cisco CMTS router.

Note There are certain QoS parameters that cannot be changed from the registered QoS parameter set and a new service class. For example, the **max-burst** value must match the originally registered in the DOCSIS configuration file, and the registered and enforced QoS service classes on the Cisco CMTS router. If the **max-burst** value differs from the registered CMTS service class and the DOCSIS configuration file, the CM might go into reject-c state, or the enforced class could fail.

The following example shows the configuration of two service classes named “BE-STM-US-1” and “BE-STM-DS-1” in a DOCSIS configuration file to define a basic set of upstream and downstream parameters:

```
03 (Net Access Control) = Yes
17 (Baseline Privacy Block)
S01 (Authorize Wait Timeout) = 10
18 (Maximum Number of CPE) = 10
24 (Upstream Service Flow Block)
S01 (Flow Reference) = 1
S04 (Service Class Name) = BE-STM-US-1
S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Block)
S01 (Flow Reference) = 2
S04 (Service Class Name) = BE-STM-DS-1
S06 (QoS Parameter Set Type) = 7
29 (Privacy Enable) = Yes
The following example shows sample cable service class
commands on the Cisco CMTS router for configuration of subscriber traffic management that
correspond to the service class names in the DOCSIS configuration file of “BE-STM-US-1” and
 “BE-STM-DS-1.” These service classes correspond to the registered service classes configured
```

```
 by the service-class registered
 command for the QoS enforce-rules shown later in this example:
cable service class 2 name BE-STM-US-1
cable service class 2 upstream
cable service class 2 max-rate 2000000
cable service class 2 max-burst 3044
cable service class 3 name BE-STM-DS-1
cable service class 3 downstream
cable service class 3 max-rate 30000000
```

The following example shows sample **cable service class** commands on the Cisco CMTS router that configure new QoS parameters for identified subscribers to limit bandwidth using the **max-rate** parameter. These service classes correspond to the enforced service classes configured by the **service-class enforced** command for the QoS enforce rules shown later in this example:

```
cable service class 102 name BEUS-1
cable service class 102 upstream
cable service class 102 max-rate 48888
cable service class 102 max-burst 3044
cable service class 103 name BEDS-1
cable service class 103 downstream
cable service class 103 max-rate 988888
```

The following example shows configuration of the corresponding enforce-rules for upstream and downstream monitoring, which identifies the registered and enforced service classes:

```
cable qos enforce-rule US-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-US-1
  service-class enforced BEUS-1
  duration 10 avg-rate 1 sample-interval 10 up enf
  enabled
!
cable qos enforce-rule DS-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-DS-1
  service-class enforced BEDS-1
  duration 10 avg-rate 1 sample-interval 10 do enf
  enabled
```

Example: Downstream Configuration

The following example shows a typical enforce-rule configuration for traffic in the downstream direction:

```
!
cable qos enforce-rule downstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 1 sample-interval 10 downstream enforce
  enabled
```

Example: Upstream Configuration

The following example shows a typical enforce-rule configuration for traffic in the upstream direction:

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
```

```
  duration 30 avg-rate 1 sample-interval 10 upstream enforce
  enabled
```

Example: Downstream and Upstream Configuration

The following example shows a typical enforce-rule configuration for traffic in both the downstream and upstream directions. Two separate rules are created, using the identical configuration, except for the keywords **upstream** and **downstream** in the **duration** command.

Note The enforce rules for the upstream and downstream directions can use either an identical configuration, or they can use their own individual configurations.

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 upstream enforce
  enabled
cable qos enforce-rule downstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 downstream enforce
  enabled
```

The following example shows an enforce-rule configuration for traffic in upstream direction. A unique penalty duration is configured for upstream, with monitoring turned on after the penalty release time.

Note For upstream direction, a unique penalty duration (120 minutes) is configured, which takes precedence over the duration configured using the penalty-period command (60 minutes). A fresh monitoring starts after the penalty release time (23:00), when all the traffic counters are reset to 0.

```
!
cable qos enforce-rule upstream_rule
  monitoring-basics peak-offpeak docsis10
  penalty-period 60 time-of-day 23:00 monitoring-on
  qos-profile registered 6
  qos-profile enforced 100
  peak-time1 10:30 duration 120 avg-rate 10 peak-time2 22:10 duration 60 avg-rate 10
sample-interval 10 penalty 120 upstream enforce
enabled
```

Example: Weekend Monitoring Configuration

The following example shows a sample configuration of peak-offpeak weekend monitoring for DOCSIS 1.0 cable modems:

```
cable qos enforce-rule monitoring
    monitoring-basics peak-offpeak docsis10
    penalty-period 60
    qos-profile registered 6
    qos-profile enforced 100
    peak-time1 10 duration 120 avg-rate 10 peak-time2 23 duration 60 avg-rate 10
sample-interval 10 upstream enforce
```

```
   weekend peak-time1 8 duration 60 avg-rate 100 peak-time2 20 duration 60 avg-rate 10000
duration 90 avg-rate 20000 sample-interval 20 downstream enforce
   enabled
```

Additional References

For additional information related to the Subscriber Traffic Management feature, refer to the following references:

Related Documents

Related Topic	Document Title
Cable commands	Cisco IOS CMTS Cable Command Reference

Standards

Standards[110]	Title
SP-RFIv1.1-I09-020830	*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1* (http://www.cablemodem.com)
draft-ietf-ipcdn-docs-rfmibv2-06	*Radio Frequency (RF) Interface Management Information Base for DOCSIS 2.0 Compliant RF Interfaces*

110 Not all supported standards are listed.

MIBs

MIBs[111]	MIBs Link
• CISCO-CABLE-QOS-MONITOR-MIB • DOSCIS-QOS-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

111 Not all supported MIBs are listed.

RFCs

RFCs[112]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support

RFCs[112]	Title
RFC 2669	Cable Device MIB

112 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Subscriber Traffic Management for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 168: Feature Information for Subscriber Traffic Management for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Subscriber Traffic Monitoring 1.0	12.2(15)BC1	This feature was introduced on the Cisco uBR7100 series routers, Cisco uBR7200 series routers, and Cisco uBR10012 router.

Feature Name	Releases	Feature Information
Subscriber Traffic Management Version 1.1	12.3(9a)BC	This feature was modified on the Cisco uBR7200 series routers and the Cisco uBR10012 router to extend the earlier STM functions and monitor a subscriber's traffic on the DOCSIS 1.1 primary service flows, and support these additional features: • Cisco STM Version 1.1 supports Cisco Broadband Troubleshooter 3.2. • Cisco STM Version 1.1 supports DOCSIS 1.1 cable modems. • Cisco STM Version 1.1 monitors and applies traffic management policies on a service-flow basis. • Cisco STM Version 1.1 increases the available monitoring window from 7 to 30 days.
Subscriber Traffic Management Version 1.1	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA to support the Cisco uBR7246VXR router, Cisco uBR7225VXR router, and Cisco uBR10012 router.

Feature Name	Releases	Feature Information
Subscriber Traffic Management Version 1.2	12.3(23)BC2	

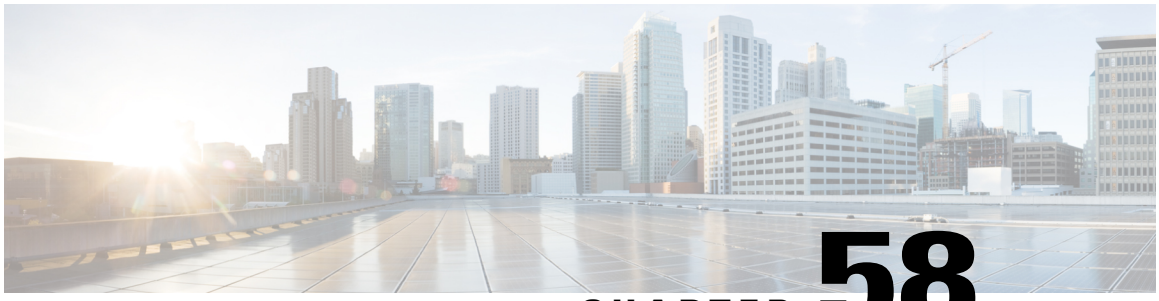
Feature Name	Releases	Feature Information
		This feature was enhanced with the following support on the Cisco uBR7246VXR and Cisco uBR10012 routers: • Support was added for the Cisco Wideband SPA (Cisco uBR10012 router only). • Support for suspension of the cable modem (CM) penalty period at a certain time of day. • Support for weekday and weekend traffic monitoring. • Support of up to 40 enforce-rules. • Support for service providers to change subscriber service classes for a particular modem using the cable modem service-class-name command. • Addition of the following SNMP objects to the CISCO-CABLE-QOS-MONITOR-MIB: ◦ ccqmCmtsEnfRulePenaltyEndTime ◦ ccqmCmtsEnfRuleWkndOff ◦ ccqmCmtsEnfRuleWkndMonDuration ◦ ccqmCmtsEnfRuleWkndAvgRate ◦ ccqmCmtsEnfRuleWkndSampleRate ◦ ccqmCmtsEnfRuleWkndFirstPeakTime ◦ ccqmCmtsEnfRuleWkndFirstDuration ◦ ccqmCmtsEnfRuleWkndFirstAvgRate ◦ ccqmCmtsEnfRuleWkndSecondPeakTime ◦ ccqmCmtsEnfRuleWkndSecondDuration ◦ ccqmCmtsEnfRuleWkndSecondAvgRate ◦ ccqmCmtsEnfRuleWkndOffPeakDuration ◦ ccqmCmtsEnfRuleWkndOffPeakAvgRate ◦ ccqmCmtsEnfRuleWkndAutoEnforce • The following commands are new or modified: ◦ **cable modem service-class-name** ◦ **penalty-period** ◦ **show cable qos enforce-rule verbose**

Feature Name	Releases	Feature Information
		◦ **weekend duration** ◦ **weekend off** ◦ **weekend peak-time1**
Subscriber Traffic Management Version 1.2	12.2(33)SCB	This feature enhancement was integrated into Cisco IOS Release 12.2(33)SCB to bring feature parity with Cisco IOS Release 12.3(23)BC2.

Feature Name	Releases	Feature Information
Subscriber Traffic Management Version 1.3	12.2(33)SCD2	This feature was enhanced with the following support on the Cisco uBR7246VXR, Cisco uBR7225VXR, and Cisco uBR10012 routers: • Support for configuring minute-level peak time—Peak time can now be configured in the hh:mm format, which enables a user to pinpoint the exact time at which monitoring should start. • Support for configuring minute-level penalty end time—Penalty end time can now be configured in the hh:mm format, which enables a user to pinpoint the exact time at which monitoring should stop. • Ability to configure a unique penalty duration for weekdays and weekends. • Ability to specify whether monitoring should be turned on after the CM is released from penalty. • Addition of the following SNMP objects to the CISCO-CABLE-QOS-MONITOR-MIB: ◦ ccqmCmtsEnfRuleFirstPeakTimeMin ◦ ccqmCmtsEnfRuleSecondPeakTimeMin ◦ ccqmCmtsEnfRuleWkndFirstPeakTimeMin ◦ ccqmCmtsEnfRuleWkndSecondPeakTimeMin ◦ ccqmCmtsEnfRulePenaltyEndTimeMin ◦ ccqmCmtsEnfRuleWkPenaltyPeriod ◦ ccqmCmtsEnfRuleWkndPenaltyPeriod ◦ ccqmCmtsEnfRuleRelTimeMonitorOn • The following commands are modified: **duration**, **peak-time1, penalty-period, show cable qos enforce-rule verbose, weekend duration, weekend peak-time1**

PART IX

Security and Cable Monitoring Features



CHAPTER 58

Cable ARP Filtering

First Published: February 14, 2008

Last Updated: February 9, 2009

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Cable ARP Filtering feature for the Cisco Cable Modem Termination System (CMTS). This feature enables service providers to filter Address Resolution Protocol (ARP) request and reply packets, to prevent a large volume of such packets from interfering with the other traffic on the cable network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Content

- Feature Information for Cable ARP Filtering on the Cisco Cable Modem Termination System, page 1602

Prerequisites for Cable ARP Filtering

The Cable ARP Filtering feature is supported on the Cisco CMTS routers in Cisco IOS software release trains 12.3BC and 12.2SC. Table 169: Cable ARP Filtering Hardware Compatibility Matrix, on page 1584 shows the hardware compatibility prerequisites for this.

Table 169: Cable ARP Filtering Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[113] **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[114] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2

113 Supports only DOCSIS 2.0 and IPv6 cable modems.
114 Supports only DOCSIS 3.0 and IPv6 cable modems.

Restrictions for Cable ARP Filtering

Cisco uBR7100 Series Restrictions

- The Cable ARP Filtering feature is not supported on the Cisco uBR7100 series universal broadband routers.

Cisco uBR10012 Router Restrictions

- The Cisco uBR10012 router maintains ARP filtering statistics on the Performance Routing Engine (PRE) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in RPR+ Redundancy, these ARP filtering statistics are reset to zero.

Cisco uBR10012 PRE modules support the Route Processor Redundancy Plus (RPR+) feature in several Cisco IOS releases. Refer to the following document for additional information:

Route Processor Redundancy Plus for the Cisco uBR10012 Universal Broadband Router

http://www.cisco.com/en/US/docs/cable/cmts/feature/u10krprp.html

- The Cable ARP Filter feature is not configurable per subinterface.

PXF ARP Filter Restrictions

- The PXF microcode must be enhanced to provide the rate limiting functionality for ARP filtering in PXF.
- ARP filtering in PXF is only supported on the Performance Routing Engine 2 (PRE2) and later versions. For more information, refer to the ARP Filtering in PXF, on page 1587.
- The ARP Filter in PXF feature is not configurable per subinterface.

Information About Cable ARP Filtering

Overview

Theft-of-service and denial-of-service (DNS) attacks have become increasingly common in cable broadband networks. In addition, virus attacks are becoming more common, and users are often unaware that their computers have become infected and are being used to continue the attacks on the network.

One sign that often appears during these attacks is an unusually high volume of Address Resolution Protocol (ARP) packets. The user or virus repeatedly issues ARP requests, trying to find the IP addresses of additional computers that might be vulnerable to attack.

ARP requests are broadcast packets, so they are broadcast to all devices on that particular network segment. In some cases, a router can also forward ARP broadcasts to an ARP proxy for further processing.

This problem is also made worse because some low-end routers commonly used by subscribers for home networks can also incorrectly respond to all ARP requests, which generates even more traffic. Until these customer premises equipment (CPE) devices can be upgraded with firmware that is compliant to the appropriate Request for Comments (RFC) specifications, service providers need to be able to deal with the incorrectly generated or forwarded traffic.

In addition, the Cisco CMTS router automatically monitors ARP traffic and enters the IP addresses found in ARP requests into its own ARP table, in the expectation that a device will eventually be found with that IP address. Unacknowledged IP addresses remain in the router's ARP table for 60 seconds, which means that a large volume of ARP traffic can fill the router's ARP table.

This process can create a large volume of ARP traffic across the network. In some situations, the volume of ARP requests and replies can become so great that it can throttle other traffic and occupy most of the Cisco CMTS router's processing time, hampering efforts by technicians to recover their network.

The router cannot use fast-switching to process ARP packets, but must instead forward them to the route processor (RP). Because of this, processing a large volume of ARP traffic can also prevent the router from handling normal traffic.

Filtering ARP Traffic

To control the volume of ARP traffic on a cable interface, you can configure the **cable arp filter** command to specify how many ARP packets are allowed per Service ID (SID) during a user-specified time period. You can configure separate thresholds for ARP request packets and for ARP reply packets.

When a cable interface is configured to filter ARP packets, it maintains a table of the number of ARP request or reply packets that have been received for each SID. If a SID exceeds the maximum number of packets during the window time period, the Cisco CMTS drops the packets until a new time period begins.

Note If using bundled cable interfaces, the Cable ARP Filtering feature is configured on the master and slave interfaces separately. This allows you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

Monitoring Filtered ARP Traffic

After ARP filtering has been enabled on a cable interface, you can then use the service **divert-rate-limit** command to display the devices that are generating excessive amounts of ARP traffic. These devices could be generating this traffic for any of the following reasons:

- Cable modems that are running software images that are either not DOCSIS-compliant or that have been hacked to allow theft-of-service attacks.
- CPE devices that are either performing a theft-of-service or denial-of-service attack, or that have been infected with a virus that is searching for other computers that can be infected.
- Routers or other devices that mistakenly reply to or forward all ARP requests.

After identifying the specific devices that are generating this traffic, you can use whatever techniques are allowed by your service level agreements (SLAs) to correct the problem.

Linksys Wireless-Broadband Router (BEFW11S4)

The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, incorrectly sends its own ARP reply packet for every ARP request packet it receives, instead of replying only to the ARP requests that are specifically for itself. Customers with these routers should upgrade the firmware to the latest revision to fix this bug. To upgrade the firmware, go to the download section on the Linksys website.

Note It is extremely important that non-compliant CPE devices be updated to firmware that correctly handles ARP and other broadcast traffic. Even one or two non-compliant devices on a segment can create a significant problem with dropped packets, impacting all of the other customers on that segment.

ARP Filtering in PXF

Cisco Release 12.3(17a)BC introduces a PXF component to the ARP filter feature. When enabled, this PXF component filters ARP packets for identified ARP offenders, decreasing the ARP punt rate and RP CPU usage. It also provides the user with clearer separation in ARP filtering by utilizing source MAC addresses instead of SIDs.

The filter logic now filters by source MAC address instead of by SID. Currently, the modem MAC addresses are excluded from having their ARPs filtered, but Multimedia Terminal Adapters (MTAs) and other non-offending CPEs can still (statistically) have ARPs filtered because all ARPs appear to come from the same SID. Therefore, filtering by source MAC address will isolate the filtering to the offensive devices. By doing so, a customer who has Voice-over-IP (VoIP) service via an MTA and an infected CPE will not have MTA issues while being contacted by the service provider in regards to the infected CPE.

ARP offenders will still be allowed to use ARP to avoid complete loss of Internet connectivity through their configured or provisioned gateway address. Because of this, it is expected that the “ARP Input” process will still show a few percentage points of CPU usage, but the net interrupt CPU usage will decrease.

Note ARP filtering in PXF is only supported on the PRE2 and later versions, and is enabled by default.

Filtering ARP Traffic in PXF

When ARP traffic in PXF is enabled, a lightweight algorithm executing on the RP is used to identify ARP offenders by the source MAC address or the SID. All offending source MAC addresses or SIDs are then programmed by the ARP Filter control module into the PXF ucode divert rate limiting module (ARP offenders are still allowed to perform ARP transactions, but only at the configured filtering rate).

Offending source MAC addresses or SIDs are filtered in PXF for a minimum of 50 minutes (ten 5-minute intervals with no occurring offenses). Utilizing the existing ARP Filter CLI tools, the cable operator can obtain enough information about the modem and CPE to contact the end user to request the necessary anti-virus software installation or firmware upgrade for the CPE.

Note If the offending device is not “repaired” or shut off, it will remain in the PXF ARP Filter indefinitely.

The PXF ARP rate limiter is designed to filter a maximum of 16,000 ARP offenders. If this pool of 16,000 filterable entities is exhausted, then the entity is filtered on the RP. The CLI statistics will distinguish mac addresses filtered on the RP verses PXF.

Because of possible mac address hash collisions, ARP offenders that cannot be programmed into the PXF ARP rate limiter will still be filtered in PXF by SID. Since the hash is done by source mac address and SID, such devices can actually moved back to mac address filtering by deleting the associated modem and forcing it back online with a new SID (this merely a possibility and is not expected to be a common practice).

ARP packets with a source mac address that is not “known” to the CMTS as a modem or CPE will be filtered by their SID in PXF. Therefore, there will never be an unusual ARP packet source that will NOT be filtered in PXF. False ARP packets with invalid operation codes will be filtered as if they are an ARP Reply.

Note ARP filtering in PXF is only supported on the PRE2 and later versions.

PXF Divert-Rate-Limit

Diverted packets sent from the forwarding processor (FP) to the route processor (RP), via the FP-to-RP interface, may encounter congestion when packets requiring diversion arrive at the FP at a faster rate than they can be transmitted to the RP. When congestion occurs, valid packets in the FP-to-RP queues will be dropped. This situation can be deliberately caused by attacks directed at the CMTS or inadvertently by faulty external hardware.

PXF Divert-Rate-Limit identifies packet streams that will cause congestion of the FP-to-RP interface. Packets in the stream are dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, preventing valid packets in other streams from being dropped.

The following diverted packets will be rate-limited:

- fwd-glean—Packets that hit a glean adjacency in the Forwarding Information Base (FIB).
- rpf-glean—Packets that hit a glean adjacency during the Reverse Path Forwarding (RPF) check.

Packets that pass rate-limiting are diverted as they normally would be. Packets that fail rate-limiting are dropped.

Rate-limiting is implemented by a token-bucket algorithm. The token-bucket algorithm requires two variables: rate and limit. Both the rate and limit are configurable via the CLI. The rate is the average number of

packets-per-second that pass the rate-limiting code. The limit can be thought of as the number of packets that will pass during an initial burst of packets.

Note The Divert-Rate-Limit feature is always on and cannot be turned off. Using the no form of the configuration CLI returns the rate-limiting parameters to their default values. During a PXF and CPU switchover or reload, the configuration is retained, but not the statistics. Therefore, after switchover, the statistics shown by the show pxf cpu statistics drl command will show zero.

fwd-glean

IP packets that hit a glean adjacency in the FIB are diverted. There are three requirements:

- RPF-check has passed (if required).
- SV-check has passed (if required).
- Forward adjacency is glean.

Packets are rate-limited based on the destination IP address. A hash on the destination IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be used and updated. The table that stores state information is large enough to make collisions rare.

rpf-glean

The RPF feature is modified to divert packets that hit a glean adjacency during the RPF check. A new divert_code will be created for this type of diverted packet. Currently, these packets are dropped.

There are four requirements:

- SV-check has passed (if required).
- RPF is enabled.
- The packet is from a non-load-balanced interface.
- RPF-adjacency is glean.

Packets are rate-limited based on the source IP address. A hash on the source IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be updated. The table that stores state information is large enough to make collisions rare.

How to Configure Cable ARP Filtering

Use the following procedures to determine whether ARP filtering is required and to configure ARP filtering on one or more cable interfaces.

Monitoring ARP Processing

Use the following steps to monitor how the router is processing ARP traffic and whether the volume of ARP packets is a potential problem.

Step 1 To discover the CPU processes that are running most often, use the **show process cpu sorted** command and look for the ARP Input process:

Example:

```
Router# show process cpu sorted

CPU utilization for five seconds: 99%/28%; one minute: 93%; five minutes: 90%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  19   139857888  44879804       3116 31.44% 28.84% 28.47%   0 ARP Input
 154    74300964  49856254       1490 20.29% 19.46% 15.78%   0 SNMP ENGINE
  91    70251936   1070352      65635  8.92%  9.62%  9.59%   0 CEF process
  56    17413012  97415887        178  3.01%  3.67%  3.28%   0 C10K BPE IP Enqu
  78    24985008  44343708        563  3.68%  3.47%  3.24%   0 IP Input
  54     6075792   6577800        923  0.90%  0.67%  0.65%   0 CMTS SID mgmt ta
...
```

In this example, the ARP Input process has used 31.44 percent of the CPU for the past five seconds. Total CPU utilization is also at 99 percent, indicating that a major problem exists on the router.

Note As a general rule, the ARP Input process should use no more than one percent of CPU processing time during normal operations. The ARP Input process could use more processing time during certain situations, such as when thousands of cable modems are registering at the same time, but if it uses more than one percent of processing time during normal operations, it probably indicates a problem.

Step 2 To monitor only the ARP processes, use the **show process cpu | include ARP** command:

Example:

```
Router# show process cpu | include ARP

  19   139857888  44879804       3116 31.44% 28.84% 28.47%   0 ARP Input
 110           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
```

Step 3 To monitor the number of ARP packets being processed, use the **show ip traffic** command.

Example:

```
Router# show ip traffic | begin ARP

ARP statistics:
  Rcvd: 11241074 requests, 390880354 replies, 0 reverse, 0 other
  Sent: 22075062 requests, 10047583 replies (2127731 proxy), 0 reverse
```

Repeat this command to see how rapidly the ARP traffic increases.

Step 4 If ARP traffic appears to be excessive, use the **show cable arp-filter** command to display ARP traffic for each cable interface, to identify the interfaces that are generating the majority of the traffic.

Example:

```
Router# show cable arp-filter Cable5/0/0

ARP Filter statistics for Cable5/0/0:
  Rcvd Replies: 177387 total, 0 unfiltered, 0 filtered
  Sent Requests For IP: 68625 total, 0 unfiltered, 0 filtered
  Sent Requests Proxied: 7969175 total, 0 unfiltered, 0 filtered
```

In the above example, the unfiltered and filtered counters show zero, which indicates that ARP filtering has not been enabled on the cable interface. After ARP filtering has been enabled with the **cable arp filter** command, you can identify the specific devices that are generating excessive ARP traffic by using the **service divert-rate-limit** command (see the Identifying the Sources of Major ARP Traffic, on page 1592).

Enabling ARP Filtering

Use the following procedure to enable ARP filtering on a particular cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 5/1`	Enters interface configuration mode for the specified cable interface.
Step 4	**cable arp filter reply-accept** *number window-size* **Example:** `Router(config-if)# cable arp filter reply-accept 2 2`	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. (The default behavior is to accept all ARP reply packets.)

	Command or Action	Purpose
Step 5	**cable arp filter request-send** *number window-size* **Example:** `Router(config-if)# cable arp filter request-send 3 1`	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. (The default behavior is to send all ARP request packets.) **Note** Repeat Step 3 through Step 5 to enable ARP filtering on other cable interfaces. Master and slave interfaces in a cable bundle must be configured separately.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Identifying the Sources of Major ARP Traffic

After you have begun filtering ARP traffic on a cable interface, use the following procedure to identify the cable modems or CPE devices that are generating or forwarding major amounts of ARP traffic.

Tip The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, has a known problem in which it incorrectly generates an ARP reply for every ARP request packet it receives. See the Linksys Wireless-Broadband Router (BEFW11S4) guide for information on how to resolve this problem.

Step 1 To discover the devices that are responsible for generating or forwarding more ARP requests on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter requests-filtered** command where *number* is the threshold value for the number of packets being generated:

Example:

show cable arp-filter cable *interface* **requests-filtered** *number*

For example, to display the devices that have generated more than 100 ARP request packets, enter the following command:

Example:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7 10.3.81.4       12407          0                    0
```

```
81    00C0.c726.6b14 10.3.81.31      743             0                       0
```

Step 2 Repeat the **show cable arp-filter** command to show how quickly the devices are generating the ARP packets.

Step 3 To discover the devices that are responsible for generating or forwarding more ARP replies on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter replies-filtered** command where *number* is the threshold value for the number of packets being generated:

Example:

show cable arp-filter cable *interface* **requests-filtered** *number*

For example, to display the devices that have generated more than 200 ARP reply packets, enter the following command:

Example:

```
Router# show cable arp-filter cable 5/0/0 replies-filtered 200

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.53b6.562f 10.11.81.16      0             0                    2358
191  0100.f31c.990a 10.11.81.6       0             0                    11290
```

Step 4 (Optional) If a particular cable modem is generating or forwarding excessive ARP replies, contact the customer to see if they are using a Linksys Wireless-B Broadband Router, Model number BEFW11S4. If so, this router could be running old firmware that is incorrectly generating excessive ARP packets, and the customer should upgrade their firmware. For more information, see the Linksys Wireless-Broadband Router (BEFW11S4) guide

Step 5 Repeat this command during each filter period (the time period you entered with the **cable arp filter** command) to show how quickly the devices are generating the ARP packets.

Step 6 (Optional) The ARP reply and request packet counters are 16-bit counters, so if a very large number of packets are being generated on an interface, these counters could wrap around to zero in a few hours or even a few minutes. Clearing the ARP counters eliminates stale information from the display and makes it easier to see the worst offenders when you suspect ARP traffic is currently creating a problem on the network.
To eliminate the modems that are not currently triggering the ARP filters and to isolate the worst current offenders, use the **clear counters cable** *interface* command to reset all of the interface counters to zero. Then the **show cable arp-filter** commands clearly identify the SIDs of the modems that are currently forwarding the most ARP traffic.

For example, the following example indicates that a number of modems are forwarding a large enough volume of ARP traffic that they have triggered the ARP packet filters:

Example:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7 10.3.81.4       8              0                    0
23   0007.0e02.b747 10.3.81.31      32             0                    0
57   0007.0e03.2c51 10.3.81.31      12407          0                    0
...
81   00C0.c726.6b14 10.3.81.31      23             0                    0
```

SID 57 shows the largest number of packets, but it is not immediately apparent if this modem is causing the current problems. After clearing the counters though, the worst offenders are easily seen:

Example:

```
Router# clear counter cable 5/1/0

Clear show interface counters on this interface [confirm] y

08:17:53.968: %CLEAR-5-COUNTERS: Clear counter on interface Cable5/1/0 by console
Router# show cable arp cable 5/1/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31      20             0                    0
81   00C0.c726.6b14 10.3.81.31      12             0                    0
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31      31             0                    0
81   00C0.c726.6b14 10.3.81.31      18             0                    0
```

Step 7 (Optional) If the Req-For-IP-Filtered column shows the majority of ARP packets, use the **show cable arp-filter ip-requests-filtered** command to display more details about the CPE device that is generating this traffic. Then use the **debug cable mac-address** and **debug cable arp filter** commands to display detailed information about this particular traffic; for example:

Example:

```
Router# show cable arp-filter c5/0/0 ip-requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
1    0007.0e03.1f59 50.3.81.3       0            37282               0
Router# debug cable mac-address 0007.0e03.1f59

Router# debug cable arp filter

Router#
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.173 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.174 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.175 prot 6 len 46 SrcP 445 DstP 445
[additional output omitted]...
```

This example shows that the CPE device at IP address 50.3.81.13 is sending packets to TCP port 445 to every IP address on the 50.3.82.0 subnet, in a possible attempt to find a computer that has Microsoft Windows file-sharing enabled.

Step 8 After determining the specific devices that are generating excessive ARP traffic, you can take whatever action is allowed by your company's service level agreements (SLAs) to correct the problem.

Examples

In this example, two cable interfaces, C5/0/0 and C7/0/0, are joined in the same bundle, which means the interfaces share the same broadcast traffic. Separate devices on each interface are generating excessive ARP traffic:

- The device at MAC address 000C.2854.72D7 on interface C7/0/0 is generating or forwarding a large volume of ARP requests. Typically, this device is a cable modem that is forwarding the ARP requests that are being generated by a CPE device behind the modem. The CPE device could be attempting a theft-of-service or denial-of-service attack, or it could be a computer that has been infected by a virus and is trying to locate other computers that can be infected.
- The device at MAC address 000C.53B6.562F on Cable 5/0/0 is responding to a large number of ARP requests, which could indicate that the device is a router that is running faulty software.

The following commands identify the device on the C7/0/0 interface that is generating the excessive ARP requests:

```
Router# show cable arp-filter c7/0/0

ARP Filter statistics for Cable7/0/0:
  Replies Rcvd: 3 total. 3 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 27906 total. 562 unfiltered, 27344 filtered
Router# show cable arp-filter c7/0/0 requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    000C.2854.72d7 50.3.81.4       62974          0                    0
```

The following commands identify the device on the C5/0/0 interface that is generating the excessive ARP replies:

```
Router# show cable arp-filter c5/0/0

ARP Filter statistics for Cable5/0/0:
  Replies Rcvd: 2400 total. 456 unfiltered, 1944 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 26 total. 26 unfiltered, 0 filtered
Router# show cable arp-filter c5/0/0 replies-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    000C.53b6.562f 50.3.81.6       0              0                    2097
```

Clearing the Packet Counters

To clear the packet counters on an interface, which includes the ARP packet counters, use the **clear counters cable** *interface* command. You can also clear the packet counters on all interfaces by using the **clear counters** command without any options. This allows you to use the **show cable arp** commands to display only the CPE devices that are currently generating the most traffic.

The following example shows the ARP packet counters being cleared:

```
Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 3278 total. 84 unfiltered, 3194 filtered
  Requests Sent For IP: 941 total. 30 unfiltered, 911 filtered
  Requests Forwarded: 941 total. 37 unfiltered, 904 filtered
```

```
Router# show cable arp cable 3/0 replies-filtered 1
Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7 50.3.72.2       1815           0                    3194
Router# show cable arp cable 3/0 requests-filtered 1
Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7 50.3.72.2       1815           0                    3194


Router# clear counter cable 3/0

Clear "show interface" counters on this interface [confirm] y

22:38:45.875: %CLEAR-5-COUNTERS: Clear counter on interface Cable3/0 by console



Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered


Router# show cable arp cable 3/0 replies-filtered 1

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered


Router# show cable arp cable 3/0 requests-filtered 1

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
```

Note The **clear counters** command clears all of the packet counters on an interface, not just the ARP packet counters.

Identifying ARP Offenders in PXF

When the PXF ARP Filter feature is enabled, use the **sho cable arp-filter** *interface* command to generate a list of ARP offenders.

The following example shows a list of ARP offenders being generated:

```
Router# show cable arp-filter ?

  Bundle  Cable Virtual bundle interface
  Cable   CMTS interface
uBR-15#sho cable arp-filter Bundle1 ?
  ip-requests-filtered  Show modems with arp request for IP packet filter count
                        at or above x
  replies-filtered      Show modems with arp reply filter count at or above x
  requests-filtered     Show modems with arp request filter count at or above x
  |                     Output modifiers
  <cr>
```

The following is a sample output from the CLI:

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  MAC Address    IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
4    0007.0e03.9cad 50.3.81.15      46           0                   0
```

```
Interface Cable7/0/0 - none
```

PRE2 Outputs in PXF

When the PXF ARP Filter feature is enabled, the PRE2 output formatting displays the modem and the CPE addresses on a single line, in addition to the following columns:

- M/S—This column shows if packets are being filtered by MAC address or SID. A majority of these columns will show MAC address.
- Rate—This column shows the packet rate for PXF-filtered packets in the last 5 minutes monitoring time window. Rate is not calculated for RP-filtered packets.
- Pro—This column will identify the processor that performed the filtering with either "RP" or "PXF." On the PRE2, it is expected that 99.9% of Pro fields will show "PXF."

The following is a sample output for an ARP request on a PRE2 in PXF:

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac        CPE IP          Modem MAC      Modem IP        M/S Rate Pro REQS
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC -    RP  46
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC 25   PXF 5012
5    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13      MAC -    RP  64000
6    -              -               0006.2854.7347 50.3.81.4       MAC 101  PXF 5122
7    -              -               0006.2854.72d7 50.3.81.11      SID -    PXF 961205
Interface Cable7/0/0 - none
```

This sample output demonstrates the following:

- SID 4 shows a CPE filtered in PXF. The threshold specified is low enough to show the packets that were filtered on the RP as the offender was being identified. A high enough threshold would not have shown the RP-filtered packets. The ARP packet rate of 25 is shown for PXF-filtered packets.
- SID 5 shows a CPE filtered on the RP. This is extremely unusual and only occurs when the maximum number of PXF-filterable entities has been reached.
- SID 6 shows a modem filtered in PXF (CPE MAC or CPE IP are not shown).
- SID 7 shows ARP packets from an "unknown" source MAC address filtered by SID in PXF.

The counts for requests, replies, and requests for IP will no longer be shown on a single line in order to keep the line concise and less than 90 characters in length.

The "REQs" column is now stated as "REPs" in the case of ARP replies. The column will show "REQ-IP" in cases involving ARP requests for IP.

Requests being sent by the CMTS due to encroaching IP packets, "ip-requests-filtered", will still be filtered on the RP and not in PXF, with Access Control Lists (ACLs) used to defeat IP-based scanning traffic, and the IP punt rate limiting feature for PRE2 used to decrease the punt rate for such traffic. The ARP Filter can still be used to perform analysis of these IP traffic streams.

PRE1 and Cisco 7246 Outputs in PXF

When the PXF ARP Filter is enabled, the PRE1 and Cisco 7246 output for the show commands is simplified to exclude all columns that do not apply.

The following is a sample output for an ARP request on a PRE1 or 7246 in PXF:

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac        CPE IP          Modem MAC      Modem IP        M/S REQs
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC 5058
5    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13      MAC 64000
6    -              -               0006.2854.7347 50.3.81.4       MAC 5122
7    -              -               0006.2854.72d7 50.3.81.11      SID 961205
Interface Cable7/0/0 - none
```

Configuring PXF Divert-Rate-Limit

Use the following procedure to configure Divert-Rate-Limit packet streams to identify potential congestion of the FP-to-RP interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • service divert-rate-limit divert-code rate limit **Example:** `Router(config)# service divert-rate-limit fib-rp-glean 10 limit 20` **Example:** `Router(config)# service divert-rate-limit fib-rpf-glean 10 limit 20`	Configures the Divert-Rate-Limit for the following packets: • fwd-glean—Packets that hit a glean adjacency in the FIB. • rpf-glean—Packets that hit a glean adjacency during the RPF check. The rate is the average number of packets-per-second that pass the rate-limiting code. The minimum rate is 1 packet-per-second and the maximum rate is 255 packets-per-second. The default rate is 20 packets-per-second. The minimum limit is 4 packets and the maximum limit is 255 packets. The default limit is 5 packets. **Note** Using the no form of the service divert-rate-limit command will reset the rate and limit to the default values.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cable ARP Filtering

This section provides the following examples of how to configure the Cable ARP Filtering features:

ARP Filtering Configuration on an Individual Cable Interface: Example

The following example shows a typical configuration of a cable interface that is configured for the Cable ARP Filtering feature:

```
!
interface Cable5/0/0
 ip address 192.168.100.1 255.255.255.0 secondary
 ip address 192.168.110.13 255.255.255.0
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 6000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000 200000
 cable upstream 0 minislot-size 16
 cable upstream 0 modulation-profile 6 7
 no cable upstream 0 shutdown
 cable upstream 1 frequency 26000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000 200000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 6 7
 no cable upstream 1 shutdown
 cable upstream 2 frequency 15008000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000 200000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 6 7
 cable upstream 2 shutdown
 cable upstream 3 spectrum-group 25
 cable upstream 3 channel-width 3200000 200000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 21008000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000 200000
 cable upstream 4 minislot-size 16
 cable upstream 4 modulation-profile 1
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 25
 cable upstream 5 channel-width 3200000 200000
 cable upstream 5 minislot-size 4
```

```
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
end
```

ARP Filtering Configuration on Bundled Cable Interfaces: Example

The following example shows a typical configuration of a cable interface bundle that is also using the Cable ARP Filtering feature. Both the master and slave interface are configured separately, allowing you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

```
!
interface Cable5/0/0
 description Master cable interface
 ip address 10.3.130.1 255.255.255.0 secondary
 ip address 10.3.131.1 255.255.255.0 secondary
 ip address 10.3.132.1 255.255.255.0 secondary
 ip address 10.3.133.1 255.255.255.0 secondary
 ip address 10.3.81.1 255.255.255.0
 ip helper-address 10.14.0.4
 load-interval 30
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
!
interface Cable7/0/0
 description Slave cable interface--Master is C5/0/0
 no ip address
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 562000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 connector 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
```

```
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable arp filter request-send 20 5
 cable arp filter reply-accept 20 5
end
```

ARP Filtering in PXF Default Configuration: Example

The following example shows the default configuration of a cable interface for the ARP Filtering in PXF feature.

```
interface Bundle1
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
end
```

Additional References

The following sections provide references related to the Cable ARP Filtering feature.

Related Documents

Related Topic	Document Title
CMTS Commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	An Ethernet Address Resolution Protocol (ARP)
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable ARP Filtering on the Cisco Cable Modem Termination System

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 170: Feature Information for the Cable ARP Filtering Feature

Feature Name	Releases	Feature Information
Cable ARP Filtering	12.2(15)BC2	This feature was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
Cable ARP Filtering	12.2(15)BC2b	The **ip-requests-filtered** option was added to the **service divert-rate-limit** command to display the specific Service IDs (SIDs) that are generating or forwarding a minimum number of ARP packets.
Cable ARP Filtering	12.3(9a)BC	Introduced optional syntax for the cable arp filter command, where number and window-size values are optional for reply-accept and request-send settings.
Cable ARP Filtering	12.3(17a)BC	The **show cable arp-filter** command was introduced for the PXF ARP Filter feature. The **service divert-rate-limit** command was introduced. Default settings changed for two commands to result as follows: • **cable arp filter request-send 3 2** • **cable arp filter reply-accept 3 2**
Cable ARP Filtering	12.2(33)SCA	This feature is integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.

CHAPTER 59

Cable Monitor and Intercept Features for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: December 02, 2012

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The Cable Monitor and Intercept features for Cisco Cable Modem Termination System (CMTS) routers provide a software solution for monitoring and intercepting traffic coming from a cable network. These features give service providers Lawful Intercept capabilities, such as those required by the Communications Assistance for Law Enforcement Act (CALEA).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Cable Monitor and Intercept Features on the Cisco CMTS Routers

The Cable Monitor and Intercept Features for the Cisco CMTS Routers is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC.

Note The cable monitor and intercept features began support in Cisco IOS Releases prior to 12.2BC; however, several of these releases and hardware have since reached End-of-Life (EOL) and therefore we are showing only some of the latest Cisco IOS software release trains in this hardware compatibility table. For more information about the complete feature history, see the Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers, on page 1621.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 171: Cable Monitor and Intercept for the Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [115]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [116]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

115 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

116 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Cable Monitor and Intercept

- The **cable intercept** command by itself does not fulfill the PacketCable requirements for Lawful Intercept capability. To meet these requirements, PacketCable operations must also be enabled and configured on the Cisco CMTS router (see the documents in the Additional References, on page 1620 for instructions on enabling PacketCable).
- For Cisco uBR10012 routers, starting from Cisco IOS Release 12.2(33)SCC, the **cable intercept** command is configured only under bundle interface and for Cisco uBR7200 series routers, **cable intercept** is allowed in Cable interface, however it is recommended to configure in Bundle interface.

Note Starting from Cisco IOS Release 12.2(33)SCH, the **cable intercept** command is not allowed to configure in Cable Interface, both in Cisco uBR7200 series and Cisco uBR10012 routers.

- The WAN interface on which packets are forwarded when using the **cable monitor** command should be used exclusively by the LAN analyzer. This interface must be an Ethernet, Fast Ethernet, Gigabit Ethernet or Ten Gigabit Ethernet interface.

- Intercepted data from the **cable intercept** command is sent to a user-specified User Datagram Port (UDP) at a user-specified IP address. The data collector at that IP address must have exclusive use of the specified UDP port.
- The interception of customer traffic is governed by local laws and the service level agreements (SLA) with those customers. Consult the proper legal authorities before intercepting and monitoring third-party traffic. Also see the documents on CALEA and Lawful Intercept in the Additional References, on page 1620.
- The Cable Monitor and Intercept feature does not support monitoring of upstream traffic if upstream channel bonding is configured on a cable interface line card.
- The Cable Monitor feature does not function correctly after a cable line card switchover. To recover from this change in functionality, re-apply the **cable monitor** command.
- The **cable monitor outbound downstream** command can be enabled:
  - only one mac-domain on a line card at a time
  - for one modular-cable or intergrated-cable interface per line card at one time
  - for one wideband-cable interface per line card at one time
- The Cable intercept feature is used to implement lawful intercept to monitor specific data or traffic streams. It is not a management tool. The information related to changes in modem states or CPE states, like DHCP information, cannot be intercepted by cable intercept feature.

Information About Cable Monitor and Intercept

Cisco CMTS routers support the following two complementary commands to intercept traffic being sent or received over a cable interface:

- **cable intercept—**Forwards copies of the traffic to and from a specific MAC address to a server at a specific IP address and UDP port. This command can be used to respond to CALEA requests from law enforcement for traffic concerning a specific user.
- **cable monitor—**Forwards copies of selected packets on the cable interface to an external LAN analyzer attached to another interface on the Cisco CMTS router. This command can help in troubleshooting network and application problems.

See the following sections for more information about these commands.

Note These commands do not monitor or intercept traffic for the purpose of preventing denial-of-service attacks and other types of network attacks. With both of these commands, the traffic continues on to its original destination, and only copies of the selected packets are forwarded to the CALEA server or LAN analyzer.

- Service Independent Intercept (SII), a superset of the existing Packet Intercept (PI) feature, is one of several systems for law enforcement to monitor traffic on the Cisco CMTS. SII differs from other systems in its ability to monitor both non-voice as well as voice traffic. Whereas the current PI feature supports the interception of UDP packets only, SII supports the interception of any legal IP protocol. In addition, because SII uses SNMP (specifically SNMPv3), its use can be hidden from other users of the CMTS.

SII requires two devices: an interception device with which to intercept monitored traffic, and a mediation device (MD) that filters and reads the intercepted traffic. Here the interception device is the Cisco CMTS, and the MD is an SNMP management workstation.

Overview of the cable intercept Command

The **cable intercept** command forwards all traffic to and from a particular MAC address on a specific cable interface to a data collection server at a particular IP address and User Datagram Protocol (UDP) port. This command examines the source and destination MAC addresses of each Ethernet frame that is transmitted over the selected cable interface, and when a match is found, a copy of the frame is encapsulated within a UDP packet and forwarded to the specified server.

Note The MAC address being intercepted is typically the MAC address of a user's CPE device (PC, Voice-over-IP phone, or so forth), not the MAC address of the cable modem.

This command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other Lawful Intercept requirements for voice communications. For specifics on CALEA Lawful Intercept, see the *PacketCable Electronic Surveillance Specification* , as listed in the Additional References, on page 1620.

This command requires that the law enforcement agency (LEA) provide a server at the specified IP address with an application that monitors the given UDP port and collects all of the data sent to that port. The choice of this application is up to the LEA. Although this application could be as simple as a packet sniffer, typically the LEA would desire a more complex application that could reconstruct the user's original data or voice traffic.

Note Before Cisco IOS Release 12.1(11b)EC, the destination server had to be within two network hops of the Cisco CMTS router. This restriction was removed in Cisco IOS Release 12.1(11b)EC, 12.2(4)BC1, and all later releases.

Note Starting from Cisco IOS Release 12.2(33)SCC, the cable intercept command is configured under bundle interface.

Overview of the Cable Monitor Command

The **cable monitor** command sends copies of packets for specific types of traffic that is sent over a particular cable interface to a LAN analyzer, for use in troubleshooting network problems. This command can select packets to be forwarded using one or more of the following parameters:

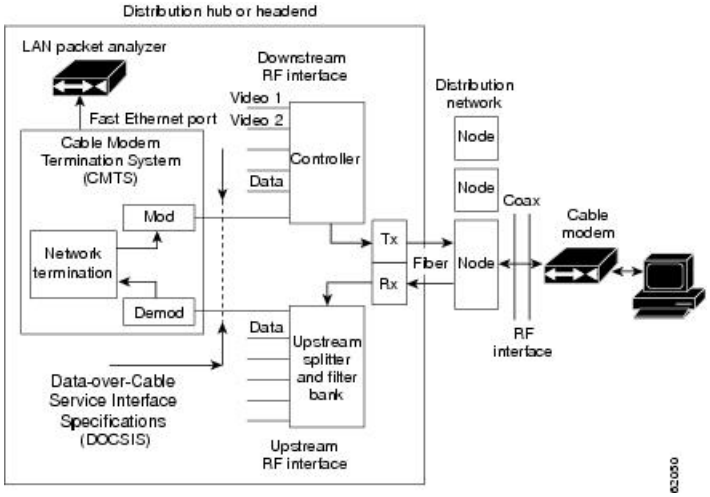
- Either incoming or outbound packets
- Packets that match an IP access list
- Packets that match a specific MAC address (source and destination)
- Packets with a specific Service ID (SID)

- When monitoring a specific SID, select only specific DOCSIS MAC-layer packet types (dynamic service packets, MAP grant packets, and MAP request packets)

In addition, the **cable monitor** command can forward full DOCSIS packets, or it can strip the DOCSIS headers and forward only the Ethernet frames. Packets can also be timestamped to aid in troubleshooting. The packets are then forwarded out of the specified Ethernet or Fast Ethernet port to the LAN analyzer for additional analysis.

The figure below illustrates a LAN packet analyzer attached to a Fast Ethernet port in a DOCSIS two-way configuration.

Figure 33: LAN Packet Analyzer in a DOCSIS Two-Way Configuration



Note The WAN port used for cable monitoring should be exclusively used by the LAN packet analyzer.

Tip When you are using the **cable monitor** command, and are including the DOCSIS header along with the Ethernet frame, it is possible that the total size of the forwarded packet could exceed the maximum allowable size for an Ethernet frame (1500 bytes), if the original Ethernet frame is at or near 1500 bytes. This is because the **cable monitor** command adds the DOCSIS header to the existing Ethernet frame. If this happens, the console displays a system message similar to the following: %LINK-4-TOOBIG:Interface Ethernet2/0, Output packet size of 1518 bytes too big This error message is typically accompanied by a traceback display. Both the error message and traceback are informational only and can be ignored. They do not indicate a traffic flow problem with the cable modem being monitored.

Note All cable modems may be captured while specifying the MAC address for a single cable modem for packets received on the upstream (**incoming**) and transmitted on the downstream (**outbound**). This issue occurs while executing the **cable monitor interface mac address** command and the MAC address of a cable modem is specified.

Overview of CISCO-TAP-MIB

There is no user-accessible CLI to support the SII feature. All interaction is implemented by means of SNMPv3, and all configurations, both for taps (SII intercepts) as well as the mediation device, are implemented by means of the CISCO-TAP-MIB.

Note At the time of publication, the Cisco IOS 12.3 BC release train does not support virtual private networks with the SII feature. The CISCO-TAP-MIB does not specify any particular VPN, so this MIB is not assigned to a particular instance of VPN routing/forwarding (VRF).

Table 172: CISCO-TAP-MIB Objects and Restrictions , on page 1611 lists the objects in the MIB, as well as restrictions for the Cisco uBR10012 CMTS other than those listed in the MIB itself.

Table 172: CISCO-TAP-MIB Objects and Restrictions

Object	Restrictions for Cisco uBR10012
cTapMediationDestAddressType	Only IPv4 is supported (ITD restriction)
cTapMediationDestAddress	
cTapMediationDestPort	
cTapMediationSrcInterface	
cTapMediationRtcpPort	Not supported (ITD restriction[117])
cTapMediationDscp	
cTapMediationDataType	
cTapMediationRetransmitType	Not supported (ITD restriction)
cTapMediationTimeout	
cTapMediationTransport	UDP only (ITD restriction)
cTapMediationNotificationEnable	
cTapMediationStatus	
cTapMediationCapabilities	
cTapStreamCapabilities	
cTapStreamIpInterface	Only if interface is cable
cTapStreamIpAddrType	IPv4 only

Object	Restrictions for Cisco uBR10012
cTapStreamIpDestinationAddress	
cTapStreamIpDestinationLength	Must be 32 (no subnets)
cTapStreamIpSourceAddress	
cTapStreamIpSourceLength	
cTapStreamIpTosByte	
cTapStreamIpTosByteMask	
cTapStreamIpFlowId	Not supported (IPv6 only)
cTapStreamIpProtocol	
cTapStreamIpDestL4PortMin	Must match ...DestL4PortMax, or zero
cTapStreamIpDestL4PortMax	Must match ...DestL4PortMin, or 65535
cTapStreamIpSourceL4PortMin	Must match ...SourceL4PortMin, or zero
cTapStreamIpSourceL4PortMax	Must match ...SourceL4PortMax, or 65535
cTapStreamIpInterceptEnable	
cTapStreamIpInterceptedPackets	
cTapStreamIpInterceptDrops	
cTapStreamIpStatus	

117 This means the restriction is across all Cisco platforms, not just Cisco CMTS platforms.

Benefits

The **cable intercept** command helps the CMTS or network administrator to:

- Comply with CALEA requirements for Lawful Intercept.
- Comply with PacketCable requirements for electronic surveillance.

Monitoring upstream and downstream data packets with the **cable monitor** command helps the CMTS or network administrator to:

- Manage network variables and understand network issues that affect application performance and functionality.
- Resolve interoperability problems.

SII, with SNMPv3, helps the CMTS or network administrator, in conjunction with law enforcement, to:

- Monitor both voice and non-voice traffic, unlike with PI.
- Hide the use of SII from other users of the Cisco CMTS.

How to Configure Cable Intercept and Monitoring Features

Configuring the Cable Intercept Feature

To enable the cable intercept feature on a particular cable interface, use the following procedure, starting in privileged EXEC mode.

Note For Cisco uBR10012 router, a maximum of 4095 MAC intercepts can be configured. This includes the MAC intercepts configured using the cable intercept command, and other lawful intercept features (such as SII). The bandwidth used by each MAC intercept is also a deciding factor for the number of MAC intercepts that can be configured. High bandwidth usage by a MAC intercept might reduce the number of MAC intercepts that can be configured.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	Do one of the following: • **interface cable** *x /y* `Router(config)# interface cable 4/0` • **interface bundle** *x* `Router(config)# interface bundle 1`	Enters cable or bundle interface configuration mode for the specified cable or bundle interface. **Note** Starting from Cisco IOS Release 12.2(33)SCC, the cable intercept command is configured under bundle interface.
Step 4	**cable intercept** *mac-address i p-address udp-port*	Enables cable interception on this cable or bundle interface with the following parameters:

	Command or Action	Purpose
	Example: `Router(config-if)# cable intercept 000C.0102.0304 10.10.10.45 8132`	• *mac-address* —Specifies the MAC address for traffic that is to be intercepted. Packets with a source or destination MAC address that matches this address are forwarded. Typically, this is the MAC address of the user's CPE device (such as a PC or VoIP phone), not the MAC address of the user's cable modem. • *ip-address*— Specifies the IP address for the data collection server that is to receive copies of the forwarded traffic. • *udp-port*—Specifies the destination UDP port number at the data collection server. The valid range is 0 to 65535 with no default. This port must be unused except by the data collection server at this IP address.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring the Cable Monitor Feature

To enable the cable traffic monitoring feature on a particular cable interface, use the following procedure, starting in privileged EXEC mode.

Note When using ACLs with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0` **Example:** `Router(config-if)#`	Enters cable interface configuration mode for the specified cable interface.
Step 4	**cable monitor incoming** | **outbound**] [**timestamp**] **interface** *interface* **access-list** *name* | *number*} | **mac-address** *address* | **sid** *sid-number* [**packet-type** {**data docsis** | **data ethernet** | **mac** [**type** *type*]}] **Example:** `Router(config-if)# cable monitor interface e1/2 mac-address 0123.4567.89ab packet-type data docsis` **Example:** `Router(config-if)#`	Enables cable monitoring on the cable interface with the following parameters: • **incoming—**(Optional) Forwards only packets being received on the upstream. • **outbound—**(Optional) Forwards only packets being transmitted on the downstream. • **timestamp—**(Optional) Appends a four-byte timestamp, in hundredths of a second, to the packets when they are forwarded to the LAN analyzer. • **interface** *interface* **—**Specifies the WAN interface on the router to which the LAN analyzer is connected. This interface should be used only by the LAN analyzer. Interface types are Ethernet, Fast Ethernet, Gigabit Ethernet, or Ten Gigabit Ethernet interface. Identify the packets to be monitored with one of the following: • **access-list—**Selects packets that match the specified access list. You can specify the access list by name or by number (1 to 2699). • **mac-address—**Specifies the MAC address for packets that should be forwarded. • **sid—**Selects packets with the specified service ID (SID). The valid range is 1 to 16384. You can configure the types of packets to be forwarded with the following options: • **packet-type—**(Optional) Selects the type of packet to be forwarded: ◦ **data docsis—**Forward only data packets as full complete DOCSIS frames.

	Command or Action	Purpose
		◦ **data ethernet—**Forward only data packets by stripping off the DOCSIS header and forwarding only the Ethernet frame. ◦ **mac—**Forwards only the MAC-layer packets. When monitoring a specific SID, you can also optionally specify the **type** option with one of the following MAC-layer message types: **dsa**, **dsc**, **dsd**, **map-grant**, **map-req**. **Note** Repeat Step 4 for each type of packet or MAC address to be monitored.
Step 5	**end** **Example:** `Router(config)# end` **Example:** `Router#`	Exits global configuration mode.

Monitoring the Cable Intercept and Monitor Features

To display information about the operation of the cable intercept and **cable monitor** commands, use the following procedures:

Displaying Information About Intercepted Traffic

To display information about what traffic is being forwarded by the **cable intercept** command, use the **show interface cable intercept** command:

```
Router#  show interface c6/0 intercept

                Destination    Destination
MAC Address     IP Address     UDP Port
00C0.0102.0DEF  10.10.10.131   7512
```

Effective with Cisco IOS Release 12.2(33)SCC, to display information about what traffic is being forwarded by the **cable intercept** command, use the **show interface bundle intercept** command:

```
Router#  show interfaces bundle 1 intercept
                MAC-based intercepts:
Source            Server           Server
MAC Address       IP Address       UDP Port
000c.0102.0304    10.10.10.45      8132
```

Displaying Information About Monitored Traffic

Note Effective with Cisco IOS Release 12.2(33)SCA the **show interface cable monitor** command is replaced by the **show interface cable cable-monitor** command.

To display information about what traffic is being sent to the external LAN analyzer by the **cable monitor** command, use the **show interface cable monitor** command:

```
Router# show interface cable 1/0 monitor
US/ Time Outbound  Flow     Flow Type      Flow  Packet MAC   MAC       Encap
DS  Stmp Interface Type     Identifier     Extn. Type   Extn. Type      Type
all  yes   Et1/0   mac-addr 0050.5462.008c yes   data   no     -        Ethernet
us   yes   Et1/0   acc-list 300            no     -     no     -          -
us   no    Et1/0   sid      2              yes   mac    yes   map-grant   -
all  no    Et1/0   acc-list rrr            no      -    no     -          -
all  no    Et1/0   mac-addr 0042.b013.008c yes   data   no     -        Ethernet
all  no    Et1/0   upstream 0              yes   data   no     -        docsis
The following is sample output from the show interface cable cable-monitor command:
```

Starting with Cisco IOS Release 12.2(33)SCA and later, use the **show interface cable cable-monitor** command to display information about what traffic is being sent to the external LAN analyzer:

```
Router# show interface cable 5/0 cable-monitor
US/ Time Outbound  Flow     Flow Type      Flow  Packet MAC   MAC       Encap
DS  Stmp Interface Type     Identifier     Extn. Type   Extn. Type      Type
us   no    Et1/2   us-port  0              yes   data   no     -        docsis
all  no    Et1/2   acc-list 103            yes   data   no     -        docsis
all  yes   Et1/2   mac-addr 0050.0000.0000 yes   mac    no     -          -
```

Configuration Examples

The following examples illustrate sample configurations of the **cableintercept** and **cablemonitor** commands and features on the Cisco CMTS:

Example: Cable Intercept Configuration

The following sample configuration shows traffic to and from MAC address 0003.e3fa.5e11 being forwarded to a data collection server at the IP address 172.18.73.189 and UDP port 9999:

```
!
interface cable 1/0
 cable monitor timestamp int fe0/0 mac-address 0002.b9ff.8c00 packet-type data ethernet
...
```

Effective from Cisco IOS Release 12.2(33)SCC, the following is the sample configuration showing traffic to and from MAC address 0003.e3fa.5e11 being forwarded to a data collection server at the IP address 172.18.73.189 and UDP port 9999:

```
!
interface bundle 1
 cable intercept 0003.e3fa.5e11 172.18.73.189 9999
...
```

Cable Monitor Examples

This section contains the following examples that illustrate the Cable Monitor feature on the Cisco CMTS:

Cable Monitor Configuration Example (MAC Address)

The following example of the **cable monitor** command on a Cisco uBR7114 router monitors packets with the MAC address of 0002.b9ff.8c00. Both upstream and downstream packets are forwarded to a LAN analyzer on the router's Fast Ethernet interface (FE0/0).

```
!
interface cable 1/0
 cable monitor timestamp int fe0/0 mac-address 0002.b9ff.8c00 packet-type data ethernet
...
```

Configuration Example for Ethernet, MAC-Layer, and DOCSIS-Data Packets

The following example of the **cable monitor** command monitors Ethernet, MAC-layer, and DOCSIS-data packets with the MAC address of 0003.e3fa.5e8f, adding a timestamp to the packets before forwarding them to the LAN analyzer.

```
!
interface Cable 3/0
 ip address 10.100.100.1 255.255.255.0
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data ethernet
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type mac
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data docsis
...
```

Cable Monitor DOCSIS Data Packets Example

This example shows sample DOCSIS packets that have been captured by the **cable monitor** command and forwarded to a LAN analyzer. The hexadecimal dump for the first packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = E2, DSAP IG Bit = 01 (Group Address)
      LLC: SSAP Address = FA, SSAP CR Bit = 00 (Command)
      LLC: I frame, N(R) = 71, N(S) = 47, POLL
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                                 ASCII
0000:c0 00 00 1c ea 1d 00 03 fe e1 a0 54 00 03 e3 fa | ...........T....
0010:5e 8f 00 0a 00 00 03 01 04
 00 00 03 00 00 00 8a | ^.............
0020:4d 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | Mn..............
0030:00 00 00 00 00 00 00 00 00 00 00 00             | ............
```

The relevant DOCSIS bytes are the following:

- Byte 0x16—Control Field. A value of 03 indicates an unnumbered information frame.
- Byte 0x17—Version of the MAC management protocol. A value of 1 indicates a DOCSIS 1.0 message and a value of 2 indicates DOCSIS 1.1 message.
- Byte 0x18—MAC message type. In this example, a value of 04 indicates a Ranging Request (RNG-REQ) message.

The hexadecimal dump of the next packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = FE, DSAP IG Bit = 00 (Individual Address
)
      LLC: SSAP Address = E0, SSAP CR Bit = 01 (Response
)
      LLC: I frame, N(R) = 42, N(S) = 80
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                                 ASCII
0000:c2 00 00 2b 00 00 00 03 e3 fa 5e 8f 00 03 fe e1 | ...+......^.....
0010:a0 54 00 19 00 00 03 01 05

00 00 03 01 01 04 00 | .T.............
0020:00 00 00 02 01 00 03 02 00 00 05 01 03 00 8a 4d | ..............M
0030:6e 00 00 00 00 00 00 00 00 00 00 00             | n...........
```

This packet has a MAC message type of 05, indicating a Ranging Response (RNG-RSP) message.

Note For complete information on the DOCSIS MAC packet format, see Chapter 6 in the DOCSIS 1.1 specification (see the Additional References, on page 1620).

Cable Monitor Timestamped Packets Example

The following example shows how to interpret the four-byte timestamp that is appended to packets that are forwarded by the **cable monitor** command when using the **timestamp** option. The following hexadecimal dump shows the 64-byte contents of the first MAP message packet being examined:

```
  0000(0000): C3
02003A 00000000  01E02F00 0001
0008...:....../.....
  0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
  0020(0032): 0061A1C1 0061A07C  00030004 FFFC4000 .a...a.|......@.
  0030(0048): 0189401F FFFC4042  0001C043 007EF4EA
 ..@...@B...C.~..
```

The relevant portions of this packet are the following:

- Byte 0—C3 indicates a MAP management message.
- Bytes 08 to 0D—Multicast address that is used to address cable modem when transmitting allocation MAP protocol data units (PDUs).
- Bytes 3C to 3F—Timestamp from the **cable monitor** command in hexadecimal (0x007EF4EA). This value is a 32-bit counter that is incremented every 10 milliseconds.

The following hexadecimal dump shows the second MAP message being forwarded:

```
  0000(0000): C302003A 00000000  01E02F00 00010008 ...:....../.....
  0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
  0020(0032): 0061A5AE 0061A469  00030004 FFFC4000 .a...a.i......@.
  0030(0048): 0189401A FFFC403D  0001C03E 007EF4EF
 ..@...@=...>.~..
```

In this example, the timestamp is 0x007EF4EF. Subtracting the two timestamps (0x007EF4EF–0x007EF4EA) produces the time difference between the two MAP messages in hundredths of a second (which in this case is a difference of 5, for a total time difference of 50 milliseconds).

Additional References

The following sections provide references related to the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
CMTS commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Common Open Policy Service (COPS)	*COPS Engine Operation on the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html
PacketCable configuration	*PacketCable and PacketCable Multimedia for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html
Using the LAN analyzer	See the documentation for the LAN analyzer or other network interception software you are using for instructions on decoding DOCSIS MAC frames. **Note** One possible software utility you can use for this purpose is the Ethereal software, which is available for Windows and Unix systems.
CALEA Information	See the Communications Assistance for Law Enforcement Act (CALEA), which was passed by the United States Congress in 1994 and is now sections 1001 to 1010 of the United States Code Title 47 (Telegraphs, Telephones, and Radiotelegraphs). Also see the information on Cisco's web site at the following URL: http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html
Lawful Intercept technology information	http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html

Standards

Standards[118]	Title
SP-RFIv1.1-I09-020830	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification

118 Not all standards supported by this release are listed.

MIBs

MIBs[119]	MIBs Link
CISCO-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

119 Not all MIBs supported by this release are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	http://www.ietf.org/rfc.html

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

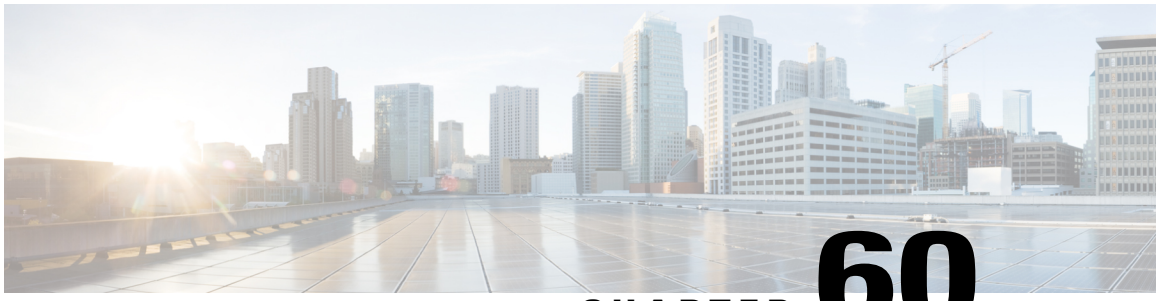
feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 173: Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Cable Intercept Feature	12.0(6)SC, 12.1(2)EC	This feature was introduced for Cisco uBR7200 series routers. The following new command was introduced: • **cable intercept**
Cable Monitor Feature	12.1(3a)EC	The **cable monitor** command was introduced for Cisco uBR7200 series routers.
Cable Monitor and Intercept Features	12.1(5)EC	Support for the **cable intercept** and **cable monitor** commands was added for the Cisco uBR7100 series routers.
Cable Intercept Feature	12.1(11b)EC	The **cable intercept** command was enhanced to allow the data collector to be more than two hops from the Cisco CMTS router.
Cable Monitor and Intercept Features	12.1(4)CX	This feature was integrated into Cisco IOS Release 12.1(4)CX. The **sid** option was added to the **cable monitor** command for DOCSIS 1.1 support.

Feature Name	Releases	Feature Information
Cable Monitor and Intercept Features	12.2(4)BC1	This feature was integrated into Cisco IOS Release 12.2(4)BC1 for the Cisco uBR7100 series, Cisco uBR7200 series, and the Cisco uBR10012 routers. However, this release does not support JIB-based cable interface line cards (such as the Cisco uBR-MC28X/U, Cisco uBR-MC16X/U, and Cisco uBR10-MC520S/U).
Service Independent Intercept	12.3(13a)BC	Support for Service Independent Intercept (SII) was introduced using the CISCO-TAP-MIB for SNMPv3. Feature support for the Cisco uBR-MC28X/U, Cisco uBR-MC16X/U, and Cisco uBR10-MC5X20S/U cable interface line cards was added to Cisco uBR7200 series and Cisco uBR10012 routers.
Cable Monitor and Intercept Features	12.3(17a)BC	• Access Control Lists are supported on the Cisco uBR10-MC5X20U/D and Cisco uBR-MC28U cable interface line cards. • Unconditional downstream sniffing enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.
Cable Monitor and Intercept Features	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 60

Cable Duplicate MAC Address Reject for the Cisco CMTS Router

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The Cable Duplicate MAC Address Reject feature is a DOCSIS 1.1-compliant security enhancement that helps to eliminate denial-of-service (DOS) attacks that are caused by cloned cable modems. A clone is presumed to be one of two physical cable modems on the same Cisco CMTS router with the same HFC interface MAC address. The cloned cable modem may be DOCSIS 1.0 or later, and may be semi-compliant or non-compliant with portions of the DOCSIS specifications.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Cable Duplicate MAC Address Reject

The Cable Duplicate MAC Address Reject feature entails the following behaviors and prerequisites on the DOCSIS-compliant network:

- The Cisco CMTS router requires that the legitimate cable modem is Baseline Privacy Interface Plus (BPI+) compliant, meaning that it can come to one of the following four online states when provisioned with a DOCSIS configuration file containing at least one BPI+ related type, length, value (TLV). For brevity, this document refers to these states as online(p_).
- The Cisco CMTS router gives priority to any cable modem that registers to the Cisco CMTS router in any of the following four states:
  - online(pt)
  - online(pk)
  - online(ptd)
  - online(pkd)

The Cisco CMTS router drops registration requests from another device that purports to use the same MAC address as an already operational modem that is in one of these four states.

Table 174: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject, on page 1627 shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 174: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20 Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [120]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [121]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

120 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

121 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Cable Duplicate MAC Address Reject

- If the cable modem is not provisioned to use DOCSIS BPI+, as characterized by not coming online with the above initialization states of online(p_), then the existing behavior of the Cisco CMTS router remains

unchanged. The Cisco CMTS router does not attempt to distinguish between two cable modems if the provisioning system does not provide a DOCSIS configuration file specifying BPI+ be enabled.

- When this feature is enabled, the Cisco CMTS router issues security breach notice in a log message in the cable logging layer2events log, or the generic log if the **cable logging layer2events** command is not configured on the Cisco CMTS router.

Information About Cable Duplicate MAC Address Reject

The Cable Duplicate MAC Address Reject feature is enabled by default on the Cisco CMTS router, and has no associated configuration commands. This feature creates a new log message, which appears in the system log by default.

This document also describes the following security features that are associated with the Cable Duplicate MAC Address Reject feature:

Early Authentication and Encryption

The Early Authentication and Encryption (EAE) feature enables the Cisco CMTS router to authenticate DOCSIS 3.0 cable modems immediately after completion of the ranging process, and encrypt all of the registration packets including DHCP and TFTP traffic. This security feature, compatible only with DOCSIS 3.0 cable modems, was introduced in Cisco IOS Release 12.2(33)SCC to help multiple service operators (MSOs) prevent theft of service.

This feature is enabled only for cable modems that initialize on a downstream channel on which the Cisco CMTS router is transmitting MAC Domain Descriptor (MDD) messages. The Cisco CMTS router uses TLV type 6 in the MDD MAC message to signal EAE to a cable modem. If this feature is enabled, only the authenticated cable modems are allowed to continue their initialization process and subsequently admitted to the network. The early authentication and encryption process involves the following:

- Authentication of the cable modem (that is the BPI+ authorization exchanges) after the ranging process.
- Traffic encryption key (TEK) exchanges for the cable modem primary Security Association Identifier (SAID).
- Encryption of IP provisioning traffic and Multipart Registration Request (REG-REQ-MP) messages during cable modem initialization.

Note When Early Authentication and Encryption is enabled, BPI will revert back to DES-56 even if the hardware supports AES-128.

EAE Enforcement Policies

The Cisco CMTS router supports the following EAE enforcement policies:

- No EAE enforcement (Policy 1)—EAE is disabled and the Cisco CMTS router cannot enforce EAE on any cable modem.
- Ranging-based EAE enforcement (Policy 2)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message.

- Capability-based EAE enforcement (Policy 3)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message in which the EAE capability flag is set using the .
- Total EAE enforcement (Policy 4)—EAE is enforced on all cable modems irrespective of the EAE capability flag status.

The EAE enforcement policies are mutually exclusive. By default, EAE is disabled on the Cisco CMTS router.

EAE Exclusion

You can exclude cable modems from EAE enforcement using the **cable privacy eae-exclude** command in the global configuration mode. Cable modems in the EAE exclusion list are always exempted from EAE enforcement. You can remove cable modems from the exclusion list using the no form of the **cable privacy eae-exclude** command.

BPI+ Security and Cloned Cable Modems

The BPI+ Security and Cloned Cable Modems feature prioritizes cable modems that are online with BPI+ security over new cable modem registration requests that use the same cable modem MAC address. As a result, the legitimate cable modem with BPI+ security certificates that match the HFC MAC address does not experience service disruption, even if a non-compliant cable modem with the same HFC MAC address attempt to register.

The cloned cable modem detection function requires that a cable modem use DOCSIS 1.1 or a later version and should be provisioned with BPI+ enabled. That is, one BPI+ type, length, value (TLV) must be included in the DOCSIS configuration file. All DOCSIS 1.0, DOCSIS 1.1, and later cable modems that are provisioned without DOCSIS BPI+ enabled continue to use the legacy DOCSIS behavior, and experience a DoS attack when a cloned cable modem appears on the Cisco CMTS router.

This cloned cable modem detection function mandates that a cable modem provisioned with BPI+ and DOCSIS 1.1 QoS must register with BPI+ and not use BPI. The commonly available non-DOCSIS-compliant cable modems contain an option to force registration in BPI as opposed to BPI+ mode even when DOCSIS 1.1 QoS and BPI+ are specified in the DOCSIS configuration file.

Logging of Cloned Cable Modems

Cloned cable modems are detected and tracked with system logging. The Logging of Cloned Cable Modem feature is enabled by default. Due to the large number of DOCSIS Layer 2 messages typically seen in a production network, a separate log is available to segregate these messages. By default, cloned cable modem messages are placed in the cable logger, cable layer2events logging. If you disable this feature using the no form of the **cable logging layer2events** command in global configuration mode, then the cloned cable modem messages are placed in the system log (syslog).

A cloned cable modem might attempt dozens of registration attempts in a short period of time. In order to suppress the number of log messages generated, the Cisco CMTS router suppresses clone detected messages for approximately 3 minutes under certain conditions.

The log message provides the cable interface and MAC address of the cable modem attempting to register when another physical modem with that same MAC address is already in a state of online(p_) elsewhere on the Cisco CMTS router.

DOCSIS 3.0 BPI+ Policy Enforcement

The DOCSIS 3.0 BPI+ Policy Enforcement feature was introduced in Cisco IOS Release 12.2(33)SCD5 to prevent cable modem MAC address cloning and theft of service. This feature enables a Cisco CMTS router to validate the MAC address of each cable modem. To enforce BPI+ on cable modems, you must configure one of the following enforcement policies per MAC domain on the router:

- 1.1 Style Configuration File Parameters and Capability (Policy 1)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. To configure this policy, the privacy support modem capability TLV (type 5.6) in the DOCSIS configuration file must be set to BPI+ support. This policy forces BPI+ on a cable modem that is BPI+ capable and provisioned with DOCSIS1.1 configuration file. A cable modem that signals these capabilities during registration is blocked from accessing the network until the modem completes BPI+ negotiation.
- 1.1 Style Configuration File Parameters (Policy 2)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. A cable modem that registers with this type of configuration file is blocked from accessing the network until the modem completes BPI+ negotiation.
- 1.1 Style Configuration File (Policy 3)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file. This means that if you provision a DOCSIS 1.1 configuration file with security disabled (privacy flag is not present in the configuration file), all DOCSIS 1.1 and 2.0 cable modems are blocked from accessing the network. Only the DOCSIS 3.0 cable modems that have security enabled implicitly will pass this check if the privacy flag is not present in the configuration file.
- Total enforcement (Policy 4)—The Cisco CMTS router enforces BPI+ on all cable modems. This means that all cable modems that do not run BPI+ are blocked from accessing the network.

Note You can configure only one enforcement policy at a time per MAC domain. If you configure one policy after another, the latest policy supersedes the already existing policy. For example, if you want Policy 2 to take over Policy 1, you can directly configure the former without disabling the latter.

These enforcement policies are implemented based on CableLabs Security Specification, CM-SP-SECv3.0-I13-100611. You can configure these enforcement policies using the **cable privacy bpi-plus-policy** command in cable interface configuration mode. The cable modems that do not comply with the configured policy can still come online but they cannot access the DOCSIS network and some dual stack cable modems may not get both the IPv4 and IPv6 addresses.

Policies 1, 2, and 3 support a mixed network of DOCSIS 1.0 (including DOCSIS Set-top Gateway), DOCSIS 1.1, and later cable modems. Policy 4 is the most effective configuration for preventing cable modem MAC address cloning as this policy enforces BPI+ on all cable modems. Policy 4 blocks all DOCSIS 1.0 cable modems as they do not register in BPI+ mode. Therefore, if Policy 4 is used, you must upgrade all authorized DOCSIS 1.0 cable modems or remove them from the network.

Note The **cable privacy bpi-plus-policy** command replaced t**he cable privacy bpi-plus-enforce c**ommand in Cisco IOS Relase12.2(33)SCD5. If you upgrade from an earlier Cisco IOS Release to Cisco IOS Release 12.2(33)SCD5 and later, the existing BPI+ enforcement configuration is disabled by default during the upgrade. You must reconfigure the BPI+ enforcement policy using the **cable privacy bpi-plus-policy** command.

BPI+ Policy Enforcement Exclusion

You can exclude cable modems (DOCSIS 1.0 and later versions) from BPI+ policy enforcement based on their MAC addresses, using the **cable privacy bpi-plus-exclude** command in global configuration mode. You can exclude a maximum of 30 cable modems per MAC domain.

How to Configure EAE and BPI+ Enforcement Features

This section provides information on how to configure the following BPI+ enforcement features:

Configuring EAE Enforcement Policies

By default, EAE is disabled on the Cisco CMTS router. You can configure EAE enforcement policies using the **cable privacy eae-policy** command in cable interface configuration mode.

Note EAE enforcement policies are enabled only for the DOCSIS 3.0 cable modems that initialize on a downstream channel.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*cable-interface-index* | *slot*/*subslot*/*cable-interface-index*} **Example:** `Router(config)# interface cable 6/0/1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**cable privacy eae-policy** {**capability-enforcement** | **disable-enforcement** | **ranging-enforcement** | **total-enforcement**} **Example:** `Router(config-if)# cable privacy eae-policy total-enforcement`	Specifies EAE enforcement policies on DOCSIS 3.0 cable modems.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Enforcing DOCSIS BPI+ Compliance on the Cisco CMTS Router

Perform these steps with the cable privacy bpi-plus-enforce command for DOCSIS BPI+ security and best performance of the Cloned Cable Modem Detection feature.

Note Beginning with Cisco IOS Release 12.2(33)SCD5, BPI+ enforcement configuration using the cable privacy bpi-plus-enforce command is not supported. In Cisco IOS Release 12.2(33)SCD5 and later, you will have to configure BPI+ enforcement policies using the cable privacy bpi-plus-policy command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` `Router(config)#`	Enters global configuration mode.
Step 3	**cable privacy bpi-plus-enforce** **Example:** `Router(config)# cable privacy bpi-plus-enforce`	Forces DOCSIS 1.1 or later cable modems to register with DOCSIS BPI+ security certificates, and not use the earlier DOCSIS BPI security.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit` `Router#`	Returns to privileged EXEC mode.
Step 5	**show cable logging** **Example:** `Router# show cable logging`	Displays whether the Layer 2 Logging feature is enabled, and displays the status of the logging buffer.

Examples enforcing DOCSIS BPI

The following example illustrates logging messages that are created with the detection of cloned cable modems. In this example, the clone modem came online just before the legitimate modem, and was taken offline according to the legacy behavior. (The cable modem was not in online (p_) state when another modem with the *same* MAC address attempted to come online.)

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been moved
from interface Cable7/0/1 to interface Cable7/0/0.
Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
 access detected at Cable7/0/0 interface
```

For additional information about this feature and supporting system log messages, see the System Messages Supporting Cable Duplicate MAC Address Reject, on page 1636.

Configuring BPI+ Enforcement Policies

The BPI+ enforcement policies are configured per MAC domain to prevent cable modem MAC address cloning and theft of service.

Before You Begin

The customer premise equipment (CPE) must use DHCP to acquire IP addresses to access the network, or the statically assigned IP addresses must be managed appropriately.

Note Only a single enforcement policy can be applied per MAC domain. If you upgrade from an earlier Cisco IOS Release to Cisco IOS Release 12.2(33)SCD5 and later, the existing BPI+ enforcement configuration is disabled by default during the upgrade. You must reconfigure BPI+ enforcement policy using the **cable privacy bpi-plus-policy** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *{slot|subslot|port |slot/port}* **Example:** `Router(config)# interface cable 5/1/0`	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable privacy bpi-plus-policy {capable-enforcement | d11-enabled-enforcement | d11-enforcement | total-enforcement}** **Example:** `Router (config-if)# cable privacy bpi-plus-policy total-enforcement`	Specifies the BPI+ enforcement policies per MAC domain.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to Privileged EXEC mode.

Troubleshooting Tips

Use the following debug commands to troubleshoot BPI+ policy enforcement configuration:

- **debug cable mac-address—**Provides debugging information about a specific cable modem.
- **debug cable bpiatp—**Enables debugging of the BPI handler.

Configuration Example for EAE and BPI+ Enforcement Policies

The following example shows how to configure an EAE enforcement policy on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 8/1/0
Router (config-if)# cable privacy eae-policy capability-enforcement
Router (config-if)# cable privacy eae-policy ranging-enforcement
Router (config-if)# cable privacy eae-policy total-enforcement
```

The following example shows how to configure a BPI+ enforcement policy at slot/subslot/port 5/1/0 on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 5/1/0
Router (config-if)# cable privacy bpi-plus-policy total-enforcement
```

Verifying EAE and BPI+ Enforcement Policies

Use the following show commands to verify EAE and BPI+ enforcement configurations:

- **show interface cable privacy**
- **show cable privacy**
- **show cable modem access-group**

To verify which EAE policy is configured on the Cisco CMTS router, use the **show interface cable privacy** command as shown in the following example:

```
Router# show interface cable 8/1/0 privacy eae-policy
EAE Configuration
 Policy: EAE Total Enforcement
```

To verify which cable modems are excluded from EAE enforcement on the Cisco CMTS router, use the **show cable privacy** command as shown in the following example:

```
Router# show cable privacy eae-exclude
EAE Exclusion List:
  MAC: 0019.474e.e80c Mask: ffff.ffff.ffff
  MAC: 0025.2eaf.6f26 Mask: ffff.ffff.ffff
```

To verify BPI+ enforcement policies, use the **show interface cable privacy** command as shown in the following example:

```
Router# show interface cable 3/1 privacy all
EAE Configuration
 Policy: EAE Enforcement disabled
KEK Configuration
 KEK lifetime: 604800
 Auth Infos: 0
 Auth Requests: 0, Auth Replies: 0
 Auth Rejects: 0, Auth Invalids: 0
 Packet Buffer Failures: 0
TEK Configuration
 TEK lifetime: 43200
```

```
 TEK Requests: 0, TEK Replies: 0
 TEK Rejects: 0, TEK Invalids: 0
 SAMap Requests: 0, SAMap Replies: 0
 SAMap Rejects: 0
Interface Configuration
 SelfSigned Trust: Untrusted
 Check Cert Validity Periods: True
```

To verify which cable modem is blocked by the Cisco CMTS router, use the show cable modem access-group command as shown in the following example. In this example, two cable modems (0025.2e2d.71fc and 0025.2e2d.7254) that do not comply with BPI+ policy requirements are blocked.

```
Router# show cable modem access-group
MAC Address IP Address Access-group
000e.9bb3.b868 19.19.1.2 N/A
0016.924f.8222 19.19.1.12 N/A
0025.2e2d.71fc 19.19.1.4 CMTS_PKT_FILTER_GROUP_255
0000.caad.109f 19.19.1.3 N/A
0025.2e2d.7254 19.19.1.14 CMTS_PKT_FILTER_GROUP_255
0000.cadb.2f56 19.19.1.6 N/A
0000.cae2.70fb 19.19.1.15 N/A
0000.caad.0da7 19.19.1.7 N/A
0022.ce89.c748 19.19.1.5 N/A
0014.04ba.c958 19.19.1.18 N/A
```

What to Do Next

The Cloned Cable Modem Detection feature relates to multiple BPI+ certificate and DOCSIS 1.1 factors.

System Messages Supporting Cable Duplicate MAC Address Reject

The following example illustrates logged events for the Cloned Cable Modem Detection feature on a Cisco uBR10012 router with PRE2 modules.

In the below scenario, there are two cable modems with MAC addresses that have been cloned:

- For MAC address 000f.66f9.48b1, the legitimate cable modem is on C5/0/0 upstream 0, and the cloned cable modem is on C7/0/0.
- For MAC address 0013.7116.e726, the legitimate cable modem is on C7/0/0 upstream 0, and the cloned cable modem is also on the same interface.
- In the below example, the CMMOVED message occurred because the cloned cable modem for MAC address 000f.66f9.48b1 came online before the legitimate cable modem.
- There is no CMMOVED message for the cable modem on interface C7/0/0 with MAC address 0013.7116.e726 because the legitimate cable modem came online with state of online(pt) before the cloned cable modem attempted to come online.

```
Dec 5 13:08:18: %UBR10000-6-CMMOVED: Cable modem 000f.66f9.48b1 has been moved from interface
 Cable7/0/0 to interface C able5/0/0.
Dec 5 13:08:44: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected o n Cable7/0/0 U0
Dec 5 13:10:48: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 000f.66f9.48b1
connection attempt rejected on Cable7/0/0 U1
Dec 5 13:12:37: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
Dec 5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
```

```
Dec  5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
 connection attempt rejected o n Cable7/0/0 U0
```

The following example of the **show cable modem** command illustrates additional cable modem information for the above scenario involving the specified MAC addresses:

```
Router# show cable modem 000f.66f9.48b1
MAC Address    IP Address      I/F       MAC          Prim RxPwr  Timing Num BPI
                                          State         Sid  (dBmv) Offset CPE Enb
000f.66f9.48b1 4.222.0.253     C5/0/0/U0 online(pt)    24    0.50  1045    1   Y
```

Additional References

Related Documents

Related Topic	Document Title
DOCSIS 1.1	DOCSIS 1.1 for the Cisco CMTS Routers
Commands on the Cisco CMTS routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

Standard	Title
CM-SP-SECv3.0-I13-100611	Data-Over-Cable Service Interface Specifications DOCSIS 3.0 Security Specification

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Duplicate MAC Address Reject

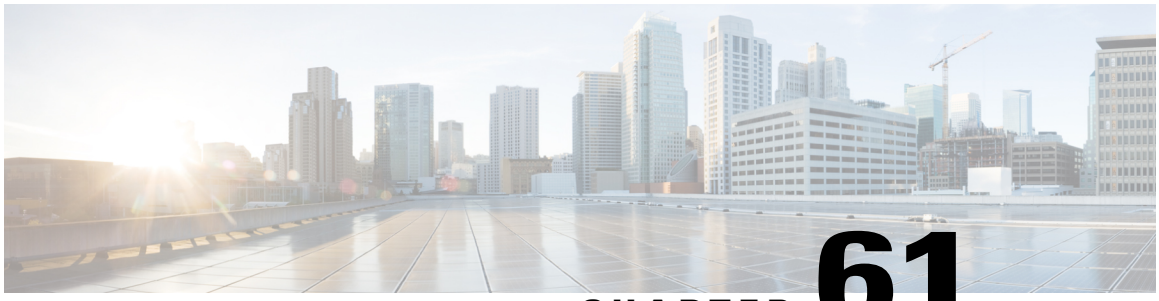
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 175: Feature Information for Cable Duplicate MAC Address Reject

Feature Name	Releases	Feature Information
BPI+ Security and Cloned Cable Modems	12.2(33)SCA	This feature prioritizes cable modems that are online with BPI+ security over new cable modem registration requests that use the same cable modem MAC address. The following sections provide information about this feature: The following commands were introduced or modified: • **cable privacy bpi-plus-enforce** • **cable logging layer2events** • **show cable logging** • **show cable modem**

Feature Name	Releases	Feature Information
Early Authentication and Encryption (EAE)	12.2(33)SCC	The EAE feature enables the Cisco CMTS router to authenticate cable modems immediately after completion of the ranging process, and encrypt all of the registration packets including DHCP and TFTP traffic. The following sections provide information about this feature: The following commands were introduced or modified: • **cable privacy eae-exclude** • **cable privacy eae-policy** • **show cable privacy** • **show interface cable privacy**
DOCSIS 3.0 BPI+ Policy Enforcement	12.2(33)SCD5	The DOCSIS 3.0 BPI+ Policy Enforcement feature was introduced in Cisco IOS Release 12.2(33)SCD5 to prevent cable modem MAC address cloning and theft of service. The following commands were introduced or modified: • **cable privacy bpi-plus-policy** • **cable privacy bpi-plus-exclude**



CHAPTER 61

DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

First Published: November 13, 2009

Last Updated: November 29, 2010

Cisco IOS Release 12.2(33)SCC provides support for certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) in Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 environment on the Cisco CMTS routers enabling you to validate the certificates issued by the certificate authority (CA) for secure transactions.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS 3.0 CRL and OCSP

- The cable modems must be DOCSIS 1.1 and above.
- Baseline Privacy Interface Plus (BPI+) must be enabled.
- The system clock on the Cisco uBR10012 universal broadband router should be set to a current date and time to ensure that system logs have the proper timestamp and to ensure that the BPI+ subsystem uses the correct timestamp for verifying cable modem digital certificates.

This table shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 176: DOCSIS 3.0 CRL and OCSP Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [122]

122 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Restrictions for DOCSIS 3.0 CRL and OCSP

The DOCSIS 3.0 CRL and OCSP have the following restrictions and limitations:

- The OCSP responder does not verify the validity of the certificate. It only verifies the revocation status of the certificate.
- When the OCSP status of a certificate is unknown to the CMTS, the certificate is treated as “valid”.
- When the CMTS fails to receive the OCSP or CRL response, the certificate is considered as “valid”.
- You cannot specify more than a single server for each protocol.

Information About DOCSIS 3.0 CRL and OCSP

The following sections describe the DOCSIS 3.0 CRL and OCSP support:

Feature Overview

CRL and OCSP are two methods used to check the revocation status of certificates that the certification authority (CA) issues.

CRL is a single signed file that lists the revocation status of certificates. The status includes the date of certificate revocation, time of CRL file creation, and time of release of the next CRL file.

OCSP is the alternative to the CRL. OCSP checks the certificate status at the external OCSP responder for each individual CA and CM certificate. The OCSP responder signs each response and the CMTS validates it.

Certificate Revocation List

Certificate revocation lists are used to check the revocation status of certificates when using a public key infrastructure (PKI) for maintaining access to servers in a network. When there is an attempt to access the server, the access action (allow or deny) is taken based on the specified CRL entry.

The CMTS retrieves the CRL files using HTTP. The retrieved files are checked with a trusted CA to ascertain the validity of the CRL file. If the CMTS cannot verify the validity of the CRL file, it discards the CRL file.

The CMTS employs the following validation process to check the validity of a CA certificate or CM certificate:

- The CMTS uses the current CRL file and attempts to retrieve the subsequent CRL file as indicated in the next-update value in the current CRL file. If the attempt fails, the CMTS continues to use the existing file and attempts to retrieve the new file at periodic intervals.
- If the next-update value is missing from the current CRL file, the CMTS uses the value configured for the CRL file.

Note The next-update value is contained in the CRL file itself.

For more details on CRL feature, refer to the What Is a CRL? section in Configuring Authorization and Revocation of Certificates in a PKI guide.

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is an alternative to Certificate Revocation Lists. It provides timely information regarding the revocation status of a digital certificate. Unlike CRL, OCSP downloads the revocation status for each CA and CM certificate individually. Because of this, any changes to the revocation states are noted quickly, but at the expense of the additional overhead of contacting the server for each certificate.

When the CMTS receives a CA certificate or CM certificate, it sends a status request to an OCSP responder using the OCSP protocol to check the revocation state of the certificate. The OCSP responder sends the response as “good”, “revoked”, or “unknown” after checking the revocation status of the certificate in its database. The CMTS uses the response from OCSP responder for the certificate validation process.

The CMTS uses the following validation process to check the validity of a CA certificate or cable modem (CM) certificate:

- The CMTS checks the OCSP response for the next-update value. If the next-update value is available, the CMTS acts as an OCSP client and caches the response status of the certificate. Next, the CMTS attempts to retrieve the revocation status of the certificate only after the time indicated in the next-update value.
- If next-update value is not available in the OCSP response, the CMTS does not cache the OCSP revocation status of the certificate and checks for the certificate validity every time a certificate validation is requested. This is a very resource-intensive method as the certificate validity is checked on a regular basis.

The CMTS sends an OCSP request when a CA certificate or CM certificate is obtained. The request is sent only when the CMTS is configured with OCSP responder information and does not posses a valid certificate status in its cache.

The CMTS treats the certificate as “valid” when:

- The CMTS is unable to retrieve the certificate status.
- The status of the certificate is “unknown”.
- The CMTS fails to receive any response from the OCSP responder.

For more details on OCSP feature, refer to the Online Certificate Status Protocol (OCSP) guide.

How to Configure DOCSIS 3.0 CRL and OCSP

This section describes the following tasks that are required to implement DOCSIS 3.0 CRL and OCSP support:

Configuring Trustpoints

This section describes how to configure trustpoints for CRL and OCSP.

Configuring a Trustpoint

This section describes how to configure trustpoints. Use the cable privacy revocation enable command at the global configuration mode to create the trustpoints and add the certificates for revocation checking.

The cable privacy revocation enable command creates the necessary trustpoints for proper DOCSIS operation. Specify the correct CRL Distribution Point and OCSP responder to configure these trustpoints.

Note IOS is based on trustpoints and the certificates configured in the system refer to this trustpoint.

For information on creating trustpoints, see the Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide .

Note To set the timeout value of CRL or OCSP response time for authorization messages, use the cable privacy revocation timeout command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation enable** **Example:** `Router(config)# cable privacy revocation enable`	Creates the trustpoints and adds the certificates for revocation checking.
Step 4	**cable privacy revocation timeout** **Example:** `Router(config)# cable privacy revocation timeout`	(Optional) Allows the CMTS to set the timeout value of OCSP response time.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to the privileged EXEC mode.

Configuring DOCSIS Trustpoints

The trustpoints for the US (DOCSIS-US-TRUSTPOINT) and EU (DOCSIS-EU-TRUSTPOINT) root certificates are created dynamically and are used to verify all the manufacturer and CM certificates.

For information on creating trustpoints, see the Configuring Trustpoints section of Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide.

Tip Use the CRL URL and the OCSP URL to add additional trustpoints. CableLabs and ComLabs also provide a public URL that contains DOCSIS root certificates signed for OCSP responses.

Configuring OCSP

Note The server specified using the ocsp url command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the OCSP response signature check, use the **cable privacy revocation ocsp skip-sig-check** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy revocation ocsp skip-sig-check**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation ocsp skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the OCSP response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring CRL

This section describes how to configure CRL. For information on Configuring CRL, see the Configuring CRLs for a Trustpoint section of Configuring Certificates document.

Note The server specified using the crl query command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the CRL response signature check, use the cable privacy revocation crl skip-sig-check command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation crl skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the CRL response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Disabling OCSP Nonce

For information on disabling OCSP Nonce, see the Disabling OCSP Nonces section of Configuring PKI Using the IPSec VPN SPA document.

Note This feature is enabled by default in IOS.

Obtaining Certificates

For information on obtaining certificates, see the Obtaining Certificates section of Configuring Certificates document.

Note The trustpoint needs a public or private keypair to sign the OCSP requests. This key should be made known to the OCSP responder to verify the request. However, signing the request is optional and the OCSP responders do not normally check the validity of the requests.

The OCSP method of checking the certificate status for each individual CA and CM certificate in real-time consumes more resources with resultant performance problems. To mitigate performance related problems, you can disable checking of the CM certificates using the **cable privacy revocation skip-cm-cert** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation skip-cm-cert** **Example:** `Router(config)# cable privacy revocation skip-cm-cert`	Allows the CMTS to disable checking of CM certificates.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring the DOCSIS 3.0 CRL and OCSP

To verify certificate and trustpoint information, perform the following steps:

Verifying Certificates

To display the certificates that are currently used on the CMTS, use the **show crypto pki certificates** command.

Verifying Certificate Revocation Lists

To display the certificate revocation lists that are currently used on the CMTS, use the **show crypto pki crls** command.

For information on verifying certificate revocation lists, see the Configuring Certificate Authorization and Revocation Settings section of the Configuring Authorization and Revocation of Certificates in a PKI document.

Configuration Examples for DOCSIS 3.0 CRL and OCSP

This section lists the following sample configurations for the DOCSIS 3.0 CRL and OCSP feature on a Cisco CMTS router:

Creating Trustpoints Examples

The following sample configuration shows typical example of a router configured to use trustpoints and optionally sets the timeout value for authorization messages:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation enable
Router(config)# cable privacy revocation timeout
Router(config)# end
```

OCSP Configuration Examples

The following sample configuration shows typical example of a router configured to skip the OCSP response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation ocsp skip-sig-check
Router(config)# end
```

CRL Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CRL response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation crl skip-sig-check
Router(config)# end
```

Obtaining Certificates Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CM certificate check:

```
Router> enable
```

```
Router# configure terminal
Router(config)# cable privacy revocation skip-cm-cert
Router(config)# end
```

Additional References

The following sections provide references related to the DOCSIS 3.0 CRL and OCSP feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Configuring Certificates	Cisco Security Appliance Command Line Configuration Guide
Security commands	Cisco IOS Security Command Reference
What is OCSP?	Configuring Authorization and Revocation of Certificates in a PKI
CMTS MIBs	Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• IF-MIB • DOCS-IF3-MIB • DOCS-SEC-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs For information on MIBs, see http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC.

RFCs

RFCs[123]	Title
RFC 3280	Internet X.509 Public Key Infrastructure CRL
RFC 2616	HTTP/1.1
RFC 2560	X.509 Internet Public Key Infrastructure OCSP

123 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

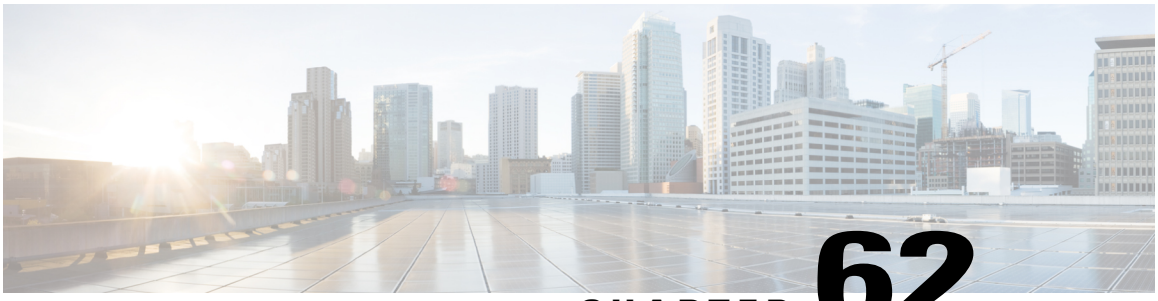
Feature Information for DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 177: Feature Information for DOCSIS 3.0 CRL and OCSP for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers	12.2(33)SCC	This feature was introduced for the Cisco uBR10012 universal broadband router. The following commands are new or modified: • **cable privacy revocation crl skip-sig-check** • **cable privacy revocation enable** • **cable privacy revocation ocsp skip-sig-check** • **cable privacy revocation skip-cm-cert** • **cable privacy revocation timeout**



CHAPTER 62

Dynamic Shared Secret for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: March 31, 2015

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Dynamic Shared Secret feature, which enables service providers to provide higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks. This feature uses randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem.

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 patented feature is designed to guarantee that all registered modems use only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for a particular modem at the time of its registration. This feature is an accepted DOCSIS standard.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Dynamic Shared Secret

The configuration of Dynamic Shared Secret feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2BC and Cisco IOS Release 12.3BC 12.2SC or later releases. Table 178: Configuring Dynamic Shared Secret on the Cisco CMTS Routers Hardware Compatibility Matrix, on page 1654 shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 178: Configuring Dynamic Shared Secret on the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco cBR-8 Converged Broadband Router	Cisco IOS-XE 3.15.0S	Cisco cBR-8 CCAP line cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE2 Cisco IOS Release 12.2(33)SCC • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [124]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V[125]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

124 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

125 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Following is a list of other important prerequisites for the Dynamic Shared Secret feature:

- The Cisco CMTS must be running Cisco IOS Release 12.2(15)BC1 or later Cisco IOS Release 12.2 BC or 12.3 BC release.
- The Dynamic Shared Secret feature supports an external provisioning server.
- The Dynamic Shared Secret feature supportsThe Dynamic Shared Secret feature supports the CMTS acting as the TFTP server (using either DOCSIS configuration files stored in Flash memory or using the internal DOCSIS configuration file editor). If you are using the CMTS as the TFTP server, you must also meet the prerequisites given in the Additional References, on page 1680.
- A cable modem must be able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.
- It is optional, but highly recommended, that you also configure a shared secret on each cable interface, and use that shared secret to create the DOCSIS configuration files for those cable modems. You can also optionally configure up to 16 secondary shared secrets on each cable interface. This is not required to use the Dynamic Shared Secret feature, but it does provide another layer of security, because the CMTS uses the manually configured shared secret to verify the original DOCSIS configuration files that it downloads from the TFTP server.

Note If a manually configured shared secret is configured, it *must* match the shared secret that was used to create the DOCSIS configuration files. If the configuration file cannot be verified against the shared secret (and any secondary shared secrets that might be configured), the CMTS does not allow any cable modems using that configuration file to come online, regardless of the Dynamic Shared Secret configuration.

- It is optional to also configure the **cable tftp-enforce** command on each cable interface to require that cable modems download their DOCSIS configuration files through the CMTS. This identifies, on a per-modem basis, those users who are attempting to bypass the shared secret checks by downloading a DOCSIS configuration file from a local TFTP server.

When the **cable tftp-enforce** command is used with the **cable dynamic-secret** command, the TFTP enforce checks are done before the dynamic shared-secret checks. If a cable modem fails to download a DOCSIS configuration file through the CMTS, it is not allowed to register, regardless of the dynamic shared-secret checks.

- The Dynamic Shared Secret feature is compatible with cable modems that are DOCSIS 1.0-, DOCSIS 1.1-, and DOCSIS 2.0-certified, which are operating in any valid DOCSIS mode.
- For full security, DOCSIS configuration files should have filenames that are at least 5 or more characters in length.
- For best performance during the provisioning of cable modems, we recommend using Cisco Network Registrar Release 3.5 or later. (See the Performance Information, on page 1663.)

Note When the Dynamic Shared Secret feature is enabled using its default configuration, a cable modem diagnostic webpage shows a scrambled name for its DOCSIS configuration file. This filename changes randomly each time that the cable modem registers with the CMTS. To change the default behavior, use the **nocrypt** option with the **cable dynamic-secret** command.

Restrictions for Dynamic Shared Secret

General Restrictions for Dynamic Shared Secret

- Shared-secret and secondary-shared-secret cannot be configured with Dynamic Shared Secret feature.
- If you configure the Dynamic Shared Secret feature on a master cable interface, you should also configure the feature on all of the corresponding slave cable interfaces.
- The Dynamic Shared Secret feature ensures that each cable modem registering with the CMTS can use only the DOCSIS configuration file that is specified by the service provider's authorized Dynamic Host Configuration Protocol (DHCP) and TFTP servers, using the DOCSIS-specified procedures.
- The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. If a cable modem is online, you must reset it, so that it reregisters, before it complies with the Dynamic Shared Secret feature.

- The DMIC lock mode uses the following behavior during a switchover event in HCCP N+1 Redundancy, commencing in Cisco IOS Release 12.3(17a)BC. All cable modems which were previously in lock mode are taken offline during a switchover event, and the prior state of locked modems is lost. If previously locked modems remain non-compliant, they will return to LOCK mode after three failed registration attempts. If the modems have become DOCSIS compliant, they will return online in the normal fashion. Refer to the SNMP Support, on page 1663 for additional information about DMIC lock mode.
- The Cisco uBR7100 series router does not support the Dynamic Shared Secret feature when running in MxU bridging mode.
- If a Broadband Access Center for Cable (BACC) provisioning server is being used, the Device Provisioning Engine (DPE) TFTP server verifies that the IP address of the TFTP client matches the expected DOCSIS cable modem IP Address. If a match is not found, the request is dropped. This functionality is incompatible with the CMTS DMIC feature. Use the no tftp verify-ip command on all BACC DPE servers to disable the verification of the requestor IP address on dynamic configuration TFTP requests. Refer to the Cisco Broadband Access Centre DPE CLI Reference in the http://www.cisco.com/c/en/us/td/docs/net_mgmt/broadband_access_center_for_cable/4-0/command/reference/DPECLIRef40.html for additional information.

Cable Modem Restrictions for Dynamic Shared Secret

DHCP Restriction for Incognito Server and Thomson Cable Modems

The Dynamic Host Configuration Protocol (DHCP) passes configuration information to DHCP hosts on a TCP/IP network. Configuration parameters and other control information are stored in the options field of the DHCP message.

When using DMIC with the Incognito DHCP server, the Incognito server must be re-configured so that the following two options are *not* sent in the DHCP message:

- *option 66* —This option is used to identify a TFTP server when the sname field in the DHCP header has been used for DHCP options. Option 66 is a variable-length field in the Options field of a DHCP message described as "an option used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options" as per RFC 2132.
- *sname field* —The sname field is a 64-octet field in the header of a DHCP message described as "optional server host name, null terminated string," as per RFC2131. A DHCP server inserts this option if the returned parameters exceed the usual space allotted for options. If this option is present, the client interprets the specified additional fields after it concludes interpretation of the standard option fields.

Note It is not compliant with DOCSIS to include both of these options in the DHCP message.

The problematic packet capture below is a DHCP offer in which both sname and option 66 are set (in this respective sequence):

```
0000  00 30 19 47 8f 00 00 d0 b7 aa 95 50 08 00 45 00
0010  01 4a 8f 50 00 00 80 11 46 30 ac 10 02 01 ac 10
0020  0a 01 00 43 00 43 01 36 0c 75 02 01 06 00 b0 a0
0030  25 01 00 00 00 00 00 00 00 00 ac 10 0a 53 00 00
0040  00 00 ac 10 0a 01 00 10 95 25 a0 b0 00 00 00 00
0050  00 00 00 00 00 00 5b 31 37 32 2e 31 36 2e 32 2e
(sname option immediately above)
```

```
0060   31 5d 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090   00 00 00 00 00 00 64 65 66 61 75 6c 74 2e 63 66
00a0   67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110   00 00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 ac
0120   10 02 01 33 04 00 06 94 0d 01 04 ff ff ff 00 02
0130   04 ff ff b9 b0 03 08 ac 10 02 fe ac 10 0a 01 04
0140   04 ac 10 02 01 07 04 ac 10 02 01 42 0a 31 37 32
(option 66 immediately above)
0150   2e 31 36 2e 32 2e 31 ff
```

When using DMIC with Incognito DHCP servers and Thomson cable modems, you must prevent both options from being sent in the DHCP offer. Use one of the following workaround methods to achieve this:

- Change the Incognito DHCP server so that it does not include the sname option as described above.
- Change the cable modem code so that sname is not prioritized above option 66, as in the problematic packet capture shown in the example above.
- Upgrade your installation of Cisco IOS to Release 12.3(9a)BC4 or a later release. These releases can exclude Thomson cable modems from the Cable dynamic secret feature by excluding the OUI setting.

Note The above method is not secure.

- Migrate to a compliant DHCP and TFTP server such as CNR. This also offers significantly higher performance.

Refer to these resources for additional DOCSIS DHCP information, or optional DHCP MAC exclusion:

- *DHCP Options and BOOTP Vendor Extensions, RFC 2132*

http://www.ietf.org/rfc/rfc2132.txt

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

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

DOCSIS Compliance

- Cable modems are assumed to be DOCSIS-compliant. If a cable modem is not fully DOCSIS-compliant, it could trigger a CMTS Message Integrity Check (MIC) failure during registration in rare circumstances. Under normal operations, however, it can be assumed that cable modems that fail the CMTS MIC check from the Dynamic Shared Secret feature are either not DOCSIS-compliant, or they might have been hacked by the end user to circumvent DOCSIS security features.

Some of the cable modems with the following OUIs have been identified as having problems with the Dynamic Shared Secret feature, depending on the hardware and software revisions:

- ◦ 00.01.03
  ◦ 00.E0.6F

- 00.02.B2

These particular cable modems can remain stuck in the init(o) MAC state and cannot come online until the Dynamic Shared Secret feature is disabled. If this problem occurs, Cisco recommends upgrading the cable modem's software to a fully compliant software revision.

Alternatively, these cable modems may be excluded from the *dynamic* secret function using the following command in global configuration mode:

cable dynamic-secret exclude

Excluding cable modems means that if a violator chooses to modify their cable modem to use one of the excluded OUIs, then the system is no longer protected. Refer to the #unique_1847.

Tip To help providers to identify non-DOCSIS compliant modems in their network, the Dynamic Shared Secret feature supports a "mark-only" option. When operating in the mark-only mode, cable modems might be able to successfully obtain higher classes of service than are provisioned, but these cable modems will be marked as miscreant in the **show cable modem** displays (with **!online**, for example). Such cable modems also display with the **show cable modem rogue** command. Service providers may decide whether those cable modems must be upgraded to DOCSIS-compliant software, or whether the end users have hacked the cable modems for a theft-of-service attack.

The following example illustrates output from a Cisco CMTS that is configured with the **cable dynamic-secret mark** command with miscreant cable modems installed. These cable modems may briefly show up as "reject(m)" for up to three registration cycles before achieving the **!online** status.

```
Router# show cable modem rogue
                                        Spoof TFTP
MAC Address    Vendor     Interface     Count Dnld Dynamic Secret
000f.0000.0133 00.0F.00   C4/0/U1       3     Yes  905B740F906B48870B3A9C5E441CDC67
000f.0000.0130 00.0F.00   C4/0/U1       3     Yes  051AEA93062A984F55B7AAC979D10901
000f.0000.0132 00.0F.00   C4/0/U2       3     Yes  FEDC1A6DA5C92B17B23AFD2BBFBAD9E1
vxr#scm | inc 000f
000f.0000.0133 4.174.4.101     C4/0/U1  !online       1     -7.00 2816    0   N
000f.0000.0130 4.174.4.89      C4/0/U1  !online       2     -6.50 2819    0   N
000f.0000.0132 4.174.4.90      C4/0/U2  !online       18    -7.00 2819    0   N
```

TFTP Restrictions

- Cable modems can become stuck in the TFTP transfer state (this is indicated as init(o) by the **show cable modem** command) in the following situation:
  - The Dynamic Shared Secret feature is enabled on the cable interface, using the **cable dynamic-secret** command. This feature applies if the cable modem is a miscreant cable modem, or if the cable modem is a DOCSIS 1.0 cable modem running early DOCSIS 1.0 firmware that has not yet been updated. This feature also applies if the TFTP server is unable to provide the cable modem's TFTP configuration file to the Cisco CMTS. This is the case, for example, when using BACC and not configuring the system to permit a TFTP request from a non-matching source IP address. The **debug cable dynamic-secret** command also shows this failure.
  - The cable modems on that interface are downloading a DOCSIS configuration file that is greater than 4 Kbytes in size. This condition applies when using a Cisco IOS release prior to 12.3(15)BC4.
  - A large number of cable modems are registering at the same time. Some or all of those cable modems could also be downloading the DOCSIS configuration file using multiple TFTP transfers

that use multiple TFTP ports on the Cisco CMTS router, and the TFTP server is unable to keep up with the rate of TFTP requests generated by the system. Some TFTP servers may be limited to the number of concurrent TFTP get requests initiated by the same source IP address per unit time, or simply unable to handle the rate of new modem registrations before cable dynamic-secret is configured. The **debug cable dynamic-secret** command shows failure to receive some files in this situation.

This situation of stuck cable modems can result in the TFTP server running out of available ports, resulting in the cable modems failing the TFTP download stage. To prevent this situation from happening, temporarily disable the Dynamic Shared Secret feature on the cable interface or reduce the size of the DOCSIS configuration file.

Individual cable modems may react better if they are power cycled after DMIC is enabled or disabled as they have trouble changing the TFTP server IP address for the DOCSIS config file. While this behavior has been indicated for older modems, it has not yet been reproduced consistently in the lab at large scale.

Information About Dynamic Shared Secret

The DOCSIS specifications require that cable modems download, from an authorized TFTP server, a DOCSIS configuration file that specifies the quality of service (QoS) and other parameters for the network session. Theft-of-service attempts frequently attempt to intercept, modify, or substitute the authorized DOCSIS configuration file, or to download the file from a local TFTP server.

To prevent theft-of-service attempts, the DOCSIS specification allows service providers to use a shared secret password to calculate the CMTS Message Integrity Check (MIC) field that is attached to all DOCSIS configuration files. The CMTS MIC is an MD5 digest that is calculated over the DOCSIS Type/Length/Value (TLV) fields that are specified in the configuration file, and if a shared secret is being used, it is used in the MD5 calculation as well.

The cable modem must include its calculation of the CMTS MIC in its registration request, along with the contents of the DOCSIS configuration file. If a user modifies any of the fields in the DOCSIS configuration file, or uses a different shared secret value, the CMTS cannot verify the CMTS MIC when the cable modem registers. The CMTS does not allow the cable modem to register, and marks it as being in the “reject(m)” state to indicate a CMTS MIC failure.

Users, however, have used various techniques to circumvent these security checks, so that they can obtain configuration files that provide premium services, and then to use those files to provide themselves with higher classes of services. Service providers have responded by changing the shared secret, implementing DOCSIS time stamps, and using modem-specific configuration files, but this has meant creating DOCSIS configuration files for every cable modem on the network. Plus, these responses would have to be repeated whenever a shared secret has been discovered.

The Dynamic Shared Secret feature prevents these types of attacks by implementing a dynamically generated shared secret that is unique for each cable modem on the network. In addition, the dynamic shared secrets are valid only for the current session and cannot be reused, which removes the threat of “replay attacks,” as well as the reuse of modified and substituted DOCSIS configuration files.

Modes of Operation

The Dynamic Shared Secret feature can operate in three different modes, depending on what action should be taken for cable modems that fail the CMTS MIC verification check:

- Marking Mode—When using the **mark** option, the CMTS allows cable modems to come online even if they fail the CMTS MIC validity check. However, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.
- Locking Mode—When the **lock** option is used, the CMTS assigns a restrictive QoS configuration to CMs that fail the MIC validity check twice in a row. You can specify a particular QoS profile to be used for locked cable modems, or the CMTS defaults to special QoS profile that limits the downstream and upstream service flows to a maximum rate of 10 kbps.

If a customer resets their CM, the CM will reregister but still uses the restricted QoS profile. A locked CM continues with the restricted QoS profile until it goes offline and remains offline for at least 24 hours, at which point it is allowed to reregister with a valid DOCSIS configuration file. A system operator can manually clear the lock on a CM by using the **clear cable modem lock** command.

This option frustrates users who are repeatedly registering with the CMTS in an attempt to guess the shared secret, or to determine the details of the Dynamic Shared Secret security system.

- Reject Mode—In the reject mode, the CMTS refuses to allow CMs to come online if they fail the CMTS MIC validity check. These cable modems are identified in the **show cable modem** displays with a MAC state of "reject(m)" (bad MIC value). After a short timeout period, the CM attempts to reregister with the CMTS. The CM must register with a valid DOCSIS configuration file before being allowed to come online. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

Note To account for possible network problems, such as loss of packets and congestion, the Cisco CMTS will allow a cable modem to attempt to register twice before marking it as having failed the Dynamic Shared Secret authentication checks.

Operation of the Dynamic Shared Secret

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 QOS parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

When a DOCSIS-compliant cable modem registers with the CMTS, it sends a DHCP request, and the DHCP server sends a DHCP response that contains the name of the DOCSIS configuration file that the cable modem should download from the specified TFTP server. The cable modem downloads the DOCSIS configuration file and uses its parameters to register with the CMTS

When the Dynamic Shared Secret feature is enabled, the CMTS performs the following when it receives the DHCP messages:

- The CMTS creates a dynamically generated shared secret.

- In the default configuration, the CMTS takes the name of the DOCSIS configuration file and generates a new, randomized filename. This randomized filename changes every time the cable modem registers, which prevents the caching of DOCSIS configuration files by cable modems that are only semi-compliant with the DOCSIS specifications. You can disable this randomization of the filename by using the **nocrypt** option with the **cable dynamic-secret** command.
- The CMTS changes the IP address of the TFTP server that the cable modem should use to the IP address of the CMTS. This informs the cable modem that it should download its configuration file from the CMTS.
- The CMTS downloads the original DOCSIS configuration file from the originally specified TFTP server so that it can modify the file to use the newly generated dynamic secret.

When the cable modem downloads the DOCSIS configuration file, it receives the modified file from the CMTS. Because this file uses the one-time-use dynamically generated shared secret, the CMTS can verify that the cable modem is using this configuration file when it attempts to register with the CMTS.

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 Although a user could attempt to circumvent these checks by downloading a DOCSIS configuration file from a local TFTP server, the cable modem would still fail the CMTS MIC verification.

To identify users who are attempting to use a locally downloaded configuration file, use the **cable tftp-enforce** command.

Interaction with Different Commands

The Dynamic Shared Secret feature works together with a number of other commands to ensure network security and integrity:

- **cable config-file—**This command enables the Cisco CMTS internal DOCSIS configuration file editor, which creates DOCSIS configuration files as part of the router's configuration. The Cisco CMTS can transmit these files to cable modems using its onboard TFTP server. The Dynamic Shared Secret feature can be used together with these DOCSIS configuration files.
- **cable qos permission—**The enforce option with this command allows you to require a cable modem to use a specific, CMTS-provided QoS profile. This command can be used with the Dynamic Shared Secret feature, but if the dynamic shared-secret lock option is used, the QoS profile specified by the **cable qos permission enforce** command takes precedence over that specified using the **lock** option.
- **cable shared-secret—**The DOCSIS specification allows service providers to use a shared-secret to ensure that cable modems are using only authorized DOCSIS configuration files.

  The Dynamic Shared Secret feature enhances this security by providing another layer of security. Cable modems must successfully pass all shared-secret checks to come online.

- **cable shared-secondary-secret—** For flexible network management, the Cisco CMTS allows you to configure additional shared secrets on a cable interface. If a cable modem fails the primary shared-secret checks, the CMTS checks the modem against the secondary shared-secrets. This allows cable providers to regularly change their shared secrets without having to update all cable modems at once. The Dynamic Shared Secret feature works together with this feature, so that if primary and secondary shared-secrets are configured, cable modems must pass at least one of those checks, as well as the dynamic shared-secret checks, before being allowed to come online.
- **cable tftp-enforce—**This command requires that cable modems download a DOCSIS configuration file over the cable interface before being allowed to come online. If a cable modem fails the TFTP-enforce checks, it is not allowed to come online. This command, along with the Dynamic Shared Secret feature, prevents the most comment theft-of-service attacks in which users try to substitute their own configuration files or try to modify the service provider's files.
- **tftp-server—**This command enables the TFTP server that is onboard the Cisco CMTS router, allowing it to deliver DOCSIS configuration files to cable modems. The DOCSIS configuration files can already be saved in the router's Flash memory, or you can create them using the router's internal DOCSIS configuration file editor. The Dynamic Shared Secret feature can be used with both types of DOCSIS configuration files and the onboard TFTP server.

Performance Information

The Dynamic Shared Secret feature does not add any additional steps to the cable modem registration process, nor does it add any additional requirements to the current provisioning systems. This feature can have either a small negative or a small positive effect on the performance of the network provisioning system, depending on the following factors:

- The provisioning system (DHCP and TFTP servers) being used
- The number of cable modems that are coming online
- The vendor and software versions of the cable modems
- The number and size of the DOCSIS configuration files

Large-scale testing has shown that the Dynamic Shared Secret feature can affect the time it takes for cable modems to come online from 5% slower to 10% faster. The most significant factor in the performance of the provisioning process is the provisioning system itself. For this reason, Cisco recommends using Cisco Network Registrar (CNR) Release 3.5 or greater, which can provide significant performance improvements over generic DHCP and TFTP servers.

The second-most important factor in the performance of cable modem provisioning is the number and size of the DOCSIS configuration files. The size of the configuration file determines how long it takes to transmit the file to the cable modem, while the number of configuration files can impact how efficiently the system keeps the files in its internal cache, allowing it to reuse identical configuration files for multiple modems.

SNMP Support

Cisco IOS Release 12.2(15)BC2 and later releases add the following SNMP support for the Dynamic Shared Secret feature:

- Adds the following MIB objects to the CISCO-DOCS-EXT-MIB:

- cdxCmtsCmDMICMode—Sets and shows the configuration of the Dynamic Shared Secret feature for a specific cable modem (not configured, mark, lock, or reject).
- cdxCmtsCmDMICLockQoS—Specifies the restrictive QoS profile assigned to a cable modem that has failed the Dynamic Shared Secret security checks, when the interface has been configured for lock mode.
- cdxCmtsCmStatusDMICTable—Lists all cable modems that have failed the Dynamic Shared Secret security checks.

- An SNMP trap (cdxCmtsCmDMICLockNotification) can be sent when a cable modem is locked for failing the Dynamic Shared Secret security checks. The trap can be enabled using the **snmp-server enable traps cable dmic-lock** command.

Note The DMIC lock mode is disabled during a switchover event in HCCP N+1 Redundancy.

System Error Messages

Cisco IOS Release 12.2(15)BC1 and later releases display the following system error messages to provide information about cable modems that have failed the CMTS Message Integrity Check (MIC) when the Dynamic Shared Secret feature is enabled.

Message

%CBR-4-CMLOCKED

The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper Dynamic Shared Secret that was used to encode it. The CMTS has, therefore, assigned a restrictive quality of service (QoS) configuration to this cable modem to limit its access to the network. The CMTS has also locked the cable modem so that it will remain locked in the restricted QoS configuration until it goes offline for at least 24 hours, at which point it is permitted to reregister and obtain normal service (assuming it is DOCSIS-compliant and using a valid DOCSIS configuration file).

This error message appears when the **cable dynamic-secret lock** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. The cable modem has been allowed to register and come online, but with a QoS configuration that is limited to a maximum rate of 10 kbps for both the upstream and downstream flows. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server. The CM cannot reregister with a different QoS profile until it has been offline for 24 hours, without attempting to register, or you have manually cleared the lock using the **clear cable modem lock** command.

Message

%CBR-4-CMMARKED

The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper dynamic shared secret that was used to encode it. The CMTS has allowed this modem to register and come online, but has marked it in the **show cable modem** displays with an exclamation point (!) so that the situation can be investigated.

This error message appears when the **cable dynamic-secret mark** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server.

Message

%CBR-4-NOCFGFILE

The CMTS could not obtain the DOCSIS configuration file for this cable modem from the TFTP server. This message occurs when the Dynamic Shared Secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Verify that the CMTS has network connectivity with the TFTP server, and that the specified DOCSIS configuration file is available on the TFTP server. Check that the DHCP server is correctly configured to send the proper configuration filename in its DHCP response to the cable modem. Also verify that the DOCSIS configuration file is correctly formatted.

This problem could also occur if the TFTP server is offline or is overloaded to the point where it cannot respond promptly to new requests. It might also be seen if the interface between the CMTS and TFTP server is not correctly configured and flaps excessively.

Note This error indicates a problem with the provisioning system outside of the Cisco CMTS. Disabling the Dynamic Shared Secret feature does not clear the fault, nor does it allow cable modems to come online. You must first correct the problem with the provisioning system.

Message

%UBR7100-4-BADCFGFILE

%UBR7200-4-BADCFGFILE

%UBR10000-4-BADCFGFILE: Modem config file [chars] at [integer]: [chars]

The DOCSIS configuration file for the cable modem failed its CMTS MIC verification, either because the MIC is missing or because the CMTS MIC failed verification with the shared secret or secondary shared secrets that have been configured for the cable interface. This message occurs when the dynamic secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Verify that the DOCSIS configuration file for the cable modem has been created using the correct shared secret value. Also verify that the DHCP server is specifying the proper configuration file for this cable modem, and that the configuration file on the TFTP server is the correct one.

Use the **show cable modem** command to display the MAC state for this particular cable modem. If the cable modem will remain in the “init(t)” state continually when the Dynamic Shared Secret feature is enabled, check for the following possible problems:

- The shared secret and secondary shared secrets that are configured on the cable interface do not match the ones that were used to create the DOCSIS configuration files. Either reconfigure the cable interface with the correct shared secret, or recreate the DOCSIS configuration files using the correct shared secret.
- The provisioning server is specifying the wrong DOCSIS configuration file for this cable modem.
- The DOCSIS configuration file on the TFTP server is either corrupted or incorrectly named.
- A user has successfully substituted their own DOCSIS configuration file into the service provider’s network.

- A cable modem has cached the DOCSIS configuration file, or a user is attempting to reuse a previously generated DOCSIS configuration file. This could also indicate a possible theft-of-service attempt by a user attempting to upload a modified DOCSIS configuration file into the operator's TFTP server.

Benefits

The Dynamic Shared Secret feature provides the following benefits to cable service providers and their partners and customers:

Improves Network Security

Service providers do not need to worry about users discovering the shared secret value and using it to modify DOCSIS configuration files to give themselves higher levels of service. Even if a user were to discover the value of a dynamically generated shared secret, the user would not be able to use that shared secret again to register.

In addition, if a manually configured shared secret is also used, the CMTS uses it to verify the DOCSIS configuration files that it receives from the TFTP server, providing MD-5 authenticated transactions between the TFTP server and the CMTS. This prevents users from bypassing the Dynamic Shared Secret feature by attempting to spoof the IP address of the provider's TFTP server.

The generic TFTP server performance and error handling on the Cisco CMTS routers has been greatly improved to support the high performance that is required for rapidly provisioning cable modems.

Flexibility in Dealing with Possible Theft-of-Service Attempts

Service providers have the option of deciding what response to take when a DOCSIS configuration file fails its CMTS MIC check: mark that cable modem and allow the user online, reject the registration request and refuse to allow the user to come online until a valid DOCSIS configuration file is used, or lock the cable modem in a restricted QoS configuration until the modem remains offline for 24 hours. Locking malicious modems is the most effective deterrent against hackers, because it provides the maximum penalty and minimum reward for any user attempting a theft-of-service attack.

No Changes to Provisioning System Are Needed

Service providers can use the Dynamic Shared Secret feature without changing their provisioning or authentication systems. Existing DOCSIS configuration files can be used unchanged, and you do not need to change any existing shared secrets.

Tip If not already done, the service provider could also install access controls that allow only the CMTS routers to download DOCSIS configuration files from the TFTP servers.

No Changes to Cable Modems Are Needed

The Dynamic Shared Secret feature does not require any end-user changes or any changes to the cable modem configuration. This feature supports any DOCSIS 1.0, DOCSIS 1.1, or DOCSIS 2.0-compatible cable modem.

Note The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. Cable modems that are already online when the feature is enabled or disabled remain online.

Simplifies Network Management

Service providers do not have to continually update the shared secrets on a cable interface whenever the files providing premium services become widely available. Instead, providers can use the same shared secret on a cable interface for significant periods of time, trusting in the Dynamic Shared Secret feature to provide unique, single-use shared secrets for each cable modem.

In addition, service providers do not have to manage unique DOCSIS configuration files for each cable modem. The same configuration file can be used for all users in the same service class, without affecting network security.

Related Features

The following features can be used with the Dynamic Shared Secret feature to enhance the overall security of the cable network.

- Baseline Privacy Interface Plus (BPI+) Authorization and Encryption—Provides a secure link between the cable modem and CMTS, preventing users from intercepting or modifying packets that are transmitted over the cable interface. BPI+ also provides for secure authorization of cable modems, using X.509 digital certificates, as well as a secure software download capability that ensures that software upgrades are not spoofed, intercepted, or altered.
- TFTP Server and Internal DOCSIS Configurator File Generator—The Cisco CMTS can act as a TFTP server, providing dynamically generated DOCSIS configuration files to cable modems. The Dynamic Shared Secret feature can be used with the DOCSIS configuration files created by the internal editor and delivered by the CMTS TFTP server.
- Shared Secrets—A shared secret can be manually configured on a cable interface using the **cable shared-secret** command. All cable modems on that interface must use DOCSIS configuration files with a CMTS MIC that has been calculated with that shared secret, before being allowed to come online. When used with the Dynamic Shared Secret feature, the CMTS uses the manually specified shared secret to verify the DOCSIS configuration files it downloads from the TFTP server, before it modifies them with the dynamically generated shared secret.

Tip When using both a manually configured shared secret and the Dynamic Shared Secret feature, when a modem's configuration file fails the manual shared secret verification, the modem remains in the "init(t)" state until it times out and reregisters. If a cable modem seems stuck in the "init(t)" state, it could be a failure of the manual shared secret verification.

- Secondary Shared Secrets—To allow service providers to change the shared secret on a cable interface, without also having to immediately change all the DOCSIS configuration files being used on that interface, a cable interface can be configured with up to 16 additional shared secrets, using the **cable shared-secondary-secret** command. When a service provider changes the primary shared secret on a cable interface, the service provider can configure the previous shared secret as a secondary secret. This allows cable modems to continue using the previous shared secret until the provider can update the configuration file with the new value.
- TFTP Enforce—To require cable modems to download a DOCSIS configuration file over the cable interface, through the CMTS, use the **cable tftp-enforce** command. This prevents a common theft-of-service attack, in which a user attempts to download a modified DOCSIS configuration file from a local TFTP server.

How to Configure the Dynamic Shared Secret Feature

The following sections describe how to enable and configure the Dynamic Shared Secret feature, to disable the feature, to manually clear a lock on a cable modem, or dynamically upgrade firmware on the cable modems.

Note All procedures begin and end at the privileged EXEC prompt ("Router#").

Enabling and Configuring the Dynamic Shared Secret Feature

This section describes how to enable and configure the Dynamic Shared Secret feature on a cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 2	**cable qos permission create** **Example:** `Router(config)# cable qos permission create` **Example:** `Router(config)#`	(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to create their own QoS profiles.
Step 3	**cable qos permission update** **Example:** `Router(config)# cable qos permission update` **Example:** `Router(config)#`	(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to update their own QoS profiles.

	Command or Action	Purpose
Step 4	**snmp-server enable traps cable dmic-lock** **Example:** `Router(config)# snmp-server enable traps cable dmic-lock` **Example:** `Router(config)#`	(Optional) Enables the sending of SNMP traps when a cable modem fails a dynamic shared-secret security check.
Step 5	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0` **Example:** `Router(config-if)#`	Enters interface configuration mode for the specified cable interface.
Step 6	**cable dynamic-secret** {**lock** [*lock-qos*] | **mark** | **reject**} [**nocrypt** **Example:** `Router(config-if)# cable dynamic-secret lock` **Example:** `Router(config-if)# cable dynamic-secret lock 90` **Example:** `Router(config-if)# cable dynamic-secret mark` **Example:** `Router(config-if)# cable dynamic-secret reject` **Example:** `Router(config-if)#`	Enables the Dynamic Shared Secret feature on the cable interface and configures it for the appropriate option: • **nocrypt—**(Optional) The Cisco CMTS does not encrypt the filenames of DOCSIS configuration files, but sends the files to CMs using their original names. • **lock—**Cable modems that fail the MIC verification are allowed online with a restrictive QoS profile. The cable modems must remain offline for 24 hours to be able to reregister with a different QoS profile. • *lock-qos* **—**(Optional) Specifies the QoS profile that should be assigned to locked cable modems. The valid range is 1 to 256, and the profile must have already been created. If not specified, locked cable modems are assigned a QoS profile that limits service flows to 10 kbps (requires Step 2 and Step 3). • **mark—**Cable modems that fail the MIC verification are allowed online but are marked in the **show cable modem** displays so that the situation can be investigated. • **reject—**Cable modems that fail the MIC verification are not allowed to register. **Note** Repeat Step 5 and Step 6 for each cable interface to be configured.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router#`	

What to Do Next

Note If you configure the Dynamic Shared Secret feature on any interface in a cable interface bundle, you should configure it on all interfaces in that same bundle.

Disabling the Dynamic Shared Secret on a Cable Interface

This section describes how to disable the Dynamic Shared Secret feature on a cable interface. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 2	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0` **Example:** `Router(config-if)#`	Enters interface configuration mode for the specified cable interface.
Step 3	**no cable dynamic-secret** **Example:** `Router(config-if)# no cable dynamic-secret`	Disables the Dynamic Shared Secret feature on the cable interface. **Note** Repeat Step 2 and Step 3 for each cable interface to be configured.

	Command or Action	Purpose
	Example: `Router(config-if)#`	
Step 4	**end** **Example:** `Router(config-if)# end` **Example:** `Router#`	Exits interface configuration mode and returns to privileged EXEC mode.

Excluding Cable Modems from the Dynamic Shared Secret Feature

This section describes how to exclude one or more cable modems from being processed by the Dynamic Shared Secret feature. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**cable dynamic-secret exclude** {**oui** *oui-id* | **modem** *mac-address*} **Example:** `Router(config)# cable dynamic-secret exclude oui 00.01.B4` `Router(config)# cable dynamic-secret exclude modem 00d0.45ba.b34b`	Excludes one or more cable modems from being processed by the Dynamic Shared Secret security checks, on the basis of their MAC addresses or OUI values: • **modem** *mac-address*—Specifies the hardware (MAC) address of one specific and individual cable modem to be excluded from the Dynamic Shared Secret feature. (You cannot specify a multicast MAC address.) • **oui** *oui-id*—Specifies the organization unique identifier (OUI) of a vendor, so that a group of cable modems from this vendor are excluded from the Dynamic Shared Secret feature. The OUI should be specified as three hexadecimal bytes separated by either periods or colons. **Note** Repeat this command for each cable modem MAC address or OUI vendor to be excluded.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Router(config)# exit`	Exits the interface configuration mode and returns to privileged EXEC mode.

Clearing the Lock on One or More Cable Modems

This section describes how to manually clear the lock on one or more cable modems. This forces the cable modems to reinitialize, and the cable modems must reregister with a valid DOCSIS configuration file before being allowed online. If you do not manually clear the lock (using the **clear cable modem lock** command), the cable modem is locked in its current restricted QoS profile and cannot reregister with a different profile until it has been offline for at least 24 hours.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear cable modem** {*mac-addr* | *ip-addr* | **all** | **oui***string* | **reject**} **lock** **Example:** `Router# clear cable modem 0001.0203.0405 lock` **Example:** `Router# clear cable modem all lock` **Example:** `Router# clear cable modem oui 00.00.0C lock` **Example:** `Router#`	Clears the lock for the cable modems, which can be identified as follows: • *mac-addr* —Specifies the MAC address for one particular cable modem to be cleared. • *ip-addr* —Specifies the IP address for one particular cable modem to be cleared. • **all**—Clears the locks on all locked cable modems. • **oui** *string* —Clears the locks on all cable modems with a vendor ID that matches the specified Organizational Unique Identifier (OUI) string. • **reject**—Clears the locks on all cable modems that are currently in the reject state (which would occur if a locked cable modem went offline and attempted to reregister before 24 hours had elapsed).

What to Do Next

Tip A cable modem can also be unlocked by manually deleting the cable modem from all CMTS internal databases, using the **clear cable modem delete** command.

Upgrading Firmware on the Cable Modems

This section describes how to upgrade firmware on cable modems by dynamically inserting the correct TLV values in the DOCSIS configuration file that is downloaded by the cable modem. The DOCSIS configuration file contains the following TLV values:

- Software Upgrade Filename (TLV 9)—Specifies the filename of the firmware.
- Upgrade IPv4 TFTP Server (TLV21)—Specifies the IPv4 address of the TFTP server from where the modem downloads the DOCSIS configuration file.
- Upgrade IPv6 TFTP Server (TLV58)—Specifies the IPv6 address of the TFTP server from where the modem downloads the DOCSIS configuration file.

Note The TFTP server addresses are inserted only when the software upgrade filename (TLV9) is specified and when the TFTP server address (TLV21/TLV58) is either not specified or set to 0.

Before You Begin

The Dynamic Shared Secret feature must be enabled first before you can upgrade the firmware on cable modems. See Enabling and Configuring the Dynamic Shared Secret Feature, on page 1668 for more information.

Note The command to enable or disable the Dynamic Shared Secret feature is available at the MAC domain level. However, the command to upgrade the firmware on cable modems is available at the global level.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	cable dynamic-secret tftp insert-upgrade-server **Example:** `Router(config)# cable dynamic-secret tftp insert-upgrade-server`	Dynamically inserts the specific IPv4 or IPv6 TLV values in the DOCSIS configuration file to complete firmware upgrade on cable modems.
Step 3	**end** **Example:** `Router(config)# end` **Example:** `Router#`	Exits the configuration mode and returns to the privileged EXEC mode.

What to Do Next

Note If you configure the Dynamic Shared Secret feature on an interface in a cable interface bundle, you should configure it on all the interfaces of that bundle.

How to Monitor the Dynamic Shared Secret Feature

This section describes the following procedures you can use to monitor and display information about the Dynamic Shared Secret feature:

Displaying Marked Cable Modems

When you configure a cable interface with the **cable dynamic-secret mark** command, cable modems that fail the dynamically generated CMTS MIC verification are allowed online, but are marked with an exclamation point (!) in the MAC state column in the **show cable modem** display. The exclamation point is also used to identify cable modems that were initially rejected, using the **cable dynamic-secret reject** command, but then reregistered using a valid DOCSIS configuration file.

For example, the following example shows that four cable modems are marked as having failed the CMTS MIC verification, but that they have been allowed online:

```
Router# show cable modems

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1     0.25    938   1    N
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online      2     -0.25   1268  0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)  13    -0.25   1920  1    N
```

```
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 !online     16    -0.50   1920  1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 !online     3     -0.50   1926  1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline     4     0.50    1929  0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 !online(pt) 22    -0.50   1929  1    N
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)  61    0.00    1925  2    N
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)  2     0.75    1925  1    N
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 online      25    -0.25   1924  1    N
0006.28f9.9d19 144.205.151.144 C6/1/1/U2 online(pt)  28    0.25    1924  1    N
0010.7bed.9b6d 144.205.151.228 C6/1/1/U2 online(pt)  59    0.25    1554  1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online      15    -0.75   1914  1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online      4     0.00    1917  1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 !online     17    0.25    1919  1    N
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)  16    0.00   !2750  1    N
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U5 online      1     0.25    1922  0    N
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)  2     0.00    1901  1    N
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)  3     0.00    1901  1    N
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)  18    -0.25   1543  1    N
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)  44    0.25    1920  21   N
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online      19    0.25    1543  1    N
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online      13    0.00    1546  1    N
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 online      12    0.50    1546  1    N
Router#
```

You can also use the **show cable modem rogue** command to display only those cable modems that have been rejected for failing the dynamic shared-secret authentication checks:

```
Router# show cable modem rogue
                                    Spoof TFTP
MAC Address    Vendor     Interface  Count Dnld Dynamic Secret
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  45494DC933F8F47A398F69EE6361B017
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  D47BCBB5494E9936D51CB0EB66EF0B0A
BBBB.7b43.aa7f Vendor2    C4/0/U5       2  No   8EB196423170B26684BF6730C099D271
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  No   DF8FE30203010001A326302430120603
BBBB.7b43.aa7f Vendor2    C4/0/U5       2  No   300E0603551D0F0101FF040403020106
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  820101002D1A264CE212A1BB6C1728B3
DDDD.7b43.aa7f Vendor4    C4/0/U5       2  Yes  7935B694DCA90BC624AC92A519C214B9
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  No   3AB096D00D56ECD07D9B7AB662451CFF
Router#
```

Displaying the Current Dynamic Secrets

In Cisco IOS Release 12.2(15)BC1, the **verbose** option for the **show cable modem** command displays the dynamically generated shared secret (a 16-byte hexadecimal value) that was used in the cable modem's previous registration cycle. The display also shows if the cable modem failed the dynamic shared-secret check or did not download the DOCSIS configuration file from the TFTP server. If a cable modem is offline, its dynamic secret is shown as all zeros.

For example, the following example shows a typical display for a single cable modem that failed the dynamic shared-secret check:

```
Router# show cable modem 00c0.73ee.bbaa verbose

MAC Address                     : 00c0.73ee.bbaa
IP Address                      : 3.18.1.6
Prim Sid                        : 2
QoS Profile Index               : 6
Interface                       : C3/0/U0
Upstream Power                  : 0.00 dBmV (SNR = 26.92 dBmV)
Downstream Power                : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                   :  2812
Initial Timing Offset           : 2812
Received Power                  :  0.00
MAC Version                     : DOC1.0
Provisioned Mode                : DOC1.0
Capabilities                    : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                  : {Max Us Sids=0, Max Ds Saids=0}
```

```
Optional Filtering Support          : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support          : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                   : 0(Max CPE IPs = 1)
CFG Max-CPE                         : 1
Flaps                               : 26(Feb 14 02:35:39)
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 6 aborts, 0 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 0 packets, 0 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 0 packets, 0 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
Active Classifiers                  : 0 (Max = NO LIMIT)
Dynamic Secret                      : A3D1028F36EBD54FDCC2F74719664D3F
Router#
```

The following example shows a typical display for a single cable modem that is currently offline (the Dynamic Secret field shows all zeros):

```
Router# show cable modem 00C0.6914.8601 verbose

MAC Address                         : 00C0.6914.8601
IP Address                          : 10.212.192.119
Prim Sid                            : 6231
QoS Profile Index                   : 2
Interface                           : C5/1/0/U3
Upstream Power                      : 0.00 dBmV (SNR = 30.19 dBmV)
Downstream Power                    : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                       : 1831
Initial Timing Offset               : 1831
Received Power                      : !-2.25
MAC Version                         : DOC1.0
Provisioned Mode                    : DOC1.0
Capabilities                        : {Frag=N, Concat=Y, PHS=N, Priv=BPI}
Sid/Said Limit                      : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support          : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support          : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                   : 4(Max CPE IPs = 4)
CFG Max-CPE                         : 4
Flaps                               : 20638(Feb 10 16:04:10)
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 108 aborts, 161 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 236222 packets, 146630868 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 9 packets, 1114 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
Active Classifiers                  : 0 (Max = NO LIMIT)
Dynamic Secret                      : 00000000000000000000000000000000
Router#
```

Note The Dynamic Secret field shown above is all zeros ("00000000000000000000000000000000"), which indicates that this cable modem is offline.

You can also use the following command to display all the dynamically generated shared secrets that are in use:

```
Router# show cable modem verbose | include Dynamic Secret

Dynamic Secret                      : 434330364346443446433038413132 37
Dynamic Secret                      : 308203E0308202C8A003020102021058
Dynamic Secret                      : 0D06092A864886F70D01010505003081
Dynamic Secret                      : 3037060355040A133044617461204F76
```

```
Dynamic Secret                  : 20496E7465726661636520537065636369
Dynamic Secret                  : 00000000000000000000000000000000
Dynamic Secret                  : 040B130C4361626C65204D6F64656D73
Dynamic Secret                  : 53204361626C65204D6F64656D20526F
Dynamic Secret                  : 7574686F72697479301E170D30313032
Dynamic Secret                  : 313233353935395A308197310B300906
Dynamic Secret                  : 0A133044617461204F76657220436162
Dynamic Secret                  : 666163652053706563696666963617469
Dynamic Secret                  : 626C65204D6F64656D73313630340603
Dynamic Secret                  : 65204D6F64656D20526F6F7420436572
Dynamic Secret                  : 747930820122300D06092A864886F70D
Dynamic Secret                  : 010100C0EF369D7BDAB0A938E6ED29C3
Dynamic Secret                  : DA398BF619A11B3C0F64912D133CFFB6
Dynamic Secret                  : FFAD6CE01590ABF5A1A0F50AC05221F2
Dynamic Secret                  : 73504BCA8278D41CAD50D9849B56552D
Dynamic Secret                  : 05F4655F2981E031EB76C90F9B3100D1
Dynamic Secret                  : F4CB0BF4A13EA9512FDE4A2A219C27E9
Dynamic Secret                  : D47BCBB5494E9936D51CB0EB66EF0B0A
Dynamic Secret                  : 8EB196423170B26684BF6730C099D271
Dynamic Secret                  : DF8FE30203010001A326302430120603
Dynamic Secret                  : 300E0603551D0F0101FF040403020106
Dynamic Secret                  : 820101002D1A264CE212A1BB6C1728B3
Dynamic Secret                  : 7935B694DCA90BC624AC92A519C214B9
Dynamic Secret                  : 3AB096D00D56ECD07D9B7AB662451CFF
Dynamic Secret                  : 92E68CFD8783D58557E3994F23A8140F
Dynamic Secret                  : 225A3B01DB67AF0C3637A765E1E7C329
Dynamic Secret                  : 2BB1E6221B6D5596F3D6F506804C995E
Dynamic Secret                  : 45494DC933F8F47A398F69EE6361B017
Router#
```

Troubleshooting Cable Modems with Dynamic Shared Secret

If a cable modem is being marked as having violated the dynamic shared secret, you can enable the following debugs to get more information about the sequence of events that is occurring:

- **debug cable mac-address** *cm-mac-addr* **verbose—**Enables detailed debugging for the cable modem with the specific MAC address.
- **debug cable tlv—**Displays the contents of Type/Length/Value messages that are sent during the registration process.
- **debug cable dynamic-secret—**Displays debugging messages about dynamic shared secret operation.
- **debug tftp server events—**Displays debugging messages for the major events that occur with the Cisco CMTS router's onboard TFTP server.
- **debug tftp server packets—**Displays a packet dump for the DOCSIS configuration files that the TFTP server downloads to a cable modem.

Tip For more information about these debug commands, see the *Cisco CMTS Debugging Commands* chapter in the Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

In addition, examine the messages in the router's log buffer for any helpful information. Use the **show logging** command to display the contents of the router's logging buffer to display these messages. You can limit the

output to a specific hour and minute by using the **begin** output modifier. For example, to display only those messages that were recorded at 12:10, give the following command:

```
Router# show logging | begin 12:10
```

Note The exact format for the **begin** output modifier depends on the timestamp you are using for your logging buffer.

Configuration Examples for Dynamic Shared Secret

This section lists a typical configuration for the Dynamic Shared Secret feature.

Note These configurations also show a shared secret and secondary secret being configured on the cable interface. This is optional but highly recommended, because it adds an additional layer of security during the registration of cable modems.

Mark Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are marked with an exclamation point (!) in the **show cable modem** displays, so that the situation can be investigated further.

```
interface cable c5/1/0
 cable dynamic-secret mark
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Lock Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are locked into a restrictive QoS configuration that limits the upstream and downstream service flows to a maximum rate of 10 kbps. A locked cable modem remains locked into the restrictive QoS configuration until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command.

```
cable qos permission create
cable qos permission update
...
interface cable c3/0
 cable dynamic-secret lock
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Note If you use the **lock** option without specifying a specific QoS profile, you must allow cable modems to create and update QoS profiles, using the **cable qos permission** command. If you do not do this and continue to use the **lock** option without specifying a particular QoS profile, locked cable modems will not be allowed to register until the lock clears or expires.

The following example is the same except that it specifies that the locked cable modem should be assigned QoS profile 90. The cable modem remains locked with this QoS profile until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command. Because a specific QoS profile is specified, you do not need to use the **cable qos permission** command.

```
interface cable c3/0
 cable dynamic-secret lock 90
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Note When a locked modem is cleared, it is automatically reset so that it reregisters with the CMTS. It is allowed online with the requested QoS parameters if it registers with a valid DOCSIS configuration that passes the Dynamic Shared Secret checks. However, the modem is locked again if it violates the DOCSIS specifications again.

Reject Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS configures the cable interface so that cable modems that fail the CMTS MIC check are rejected and not allowed to register. The cable modem must reregister using a DOCSIS configuration file with a CMTS MIC that matches one of the shared secret or secondary secret values. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

```
interface cable c3/0
 cable dynamic-secret reject
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Disabled Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7100 series router disables the Dynamic Shared Secret feature. In this configuration, the CMTS uses the shared secret and secondary shared secret values unchanged when verifying the CMTS MIC value for each DOCSIS configuration file.

```
interface cable c1/0
 no cable dynamic-secret
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Additional References

For additional information related to Dynamic Shared Secret, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS command reference	Cisco IOS Release 12.2 Command References http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Configuring DOCSIS 1.1 on the Cisco CMTS	"DOCSIS 1.1 for the Cisco CMTS Routers" in the *Cisco IOS CMTS Cable Software Configuration Guide* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis11.html
Cisco Network Registrar End User Guides	Cisco Network Registrar user guides http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_list.html
Cisco Broadband Access Center DPE CLI Reference, 2.7.1	Cisco Broadband Access Center DPE CLI REference, 2.7.1 http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/2.7.1/command/reference/cli.html

Standards

Standards[126]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

126 Not all supported standards are listed.

MIBs

MIBs[127]	MIBs Link
No new or modified MIB objects are supported by the Dynamic Shared Secret feature. • CISCO-DOCS-EXT-MIB—Includes attributes to configure the Dynamic Shared Secret feature and to generate traps when a cable modem fails the shared-secret security checks.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

127 Not all supported MIBs are listed.

RFCs

RFCs[128]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

128 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

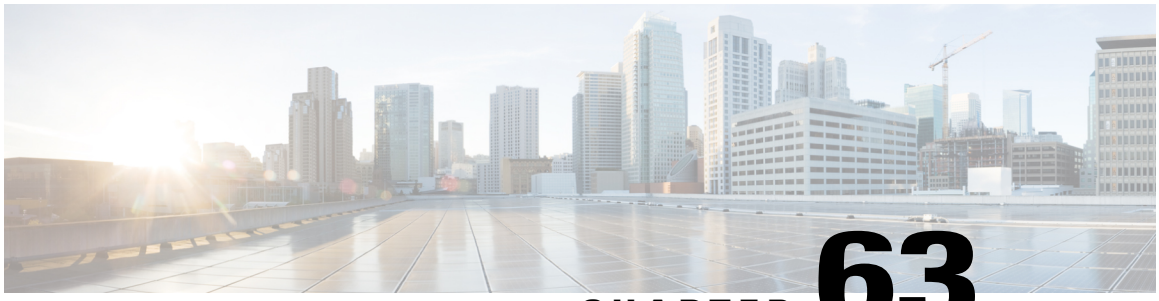
Feature Information for Dynamic Shared Secret

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 179: Feature Information for Dynamic Shared Secret

Feature Name	Releases	Feature Information
Dynamic Shared Secret	12.2(15)BC1	This feature was introduced.
Changing Default Behavior of Dynamic Shared Secret	12.2(15)BC1b	Support for the **nocrypt** option was added to the **cable dynamic-secret** command.
SNMP support for the Dynamic Shared Secret	12.2(15)BC2	SNMP support for the Dynamic Shared Secret feature was added to CISCO-DOCS-EXT-MIB, and a new option (**dmic-lock**) was added to the **snmp-server enable traps cable** command.
Excluding Cable Modems from Dynamic Shared Secret	12.3(9a)BC	The **cable dynamic-secret exclude** command was added to allow specific cable modems to be excluded from the Dynamic Shared Secret feature.
DMIC lock mode	12.3(17a)BC	The DMIC lock mode behavior is revised to support additional security during N+1 Redundancy switchover events. Refer to Restrictions for Dynamic Shared Secret, on page 1656 for additional information.
Dynamic Insertion of TFTP Server TLV for CM Firmware Upgrade	12.2(33)SCD2	The cable dynamic-secret tftp insert-upgrade-server command was added to support dynamic insertion of the TFTP server address in the DOCSIS configuration file.



CHAPTER 63

Cable DHCP Leasequery

First Published: February 14, 2008

Last Updated: November 29, 2010

This document describes the Dynamic Host Configuration Protocol (DHCP) Leasequery feature on the Cisco cable modem termination system (CMTS) router.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

- Feature Information for Cable DHCP Leasequery , page 1693

Prerequisites for Cable DHCP Leasequery

- The Cisco CMTS router must be running Cisco IOS Release 12.2(15)BC1d or Cisco IOS Release12.2(15)BC2b or Cisco IOS Release 12.2(33)SCA or a later release.
- You must configure a cable interface with the **cable source-verify dhcp** command and the **no cable arp** command before the Cisco CMTS router can enable DHCP Leasequery. Lease queries are sent to the DHCP server or to a configured alternate server.

To divert DHCP Leasequeries to a specific server, you must use the cable **source-verify dhcp server** ipaddress command and the **no cable arp** command before the Cisco CMTS router is enabled for DHCP Leasequery. Only one alternate server may be configured.

- You must configure the **cable ipv6 pd-route** command when IPv6 Customer Premise Equipment (CPE) routers are deployed on the Cisco CMTS router.

Restrictions for Cable DHCP Leasequery

- Leasequeries are sent to the DHCP server unless an alternate server is configured.
- Only one alternate server can be configured.
- Users are responsible for the synchronization of the DHCP server and the configured alternate server.
- If the configured alternate server fails, leasequery requests are *not* returned to the DHCP server.
- Only one IA_IADDR is supported per client. If the leasequery returns multiple results, only the IA_ADDR matching the query is added to the Cisco CMTS subscriber database.
- The Cisco CMTS will not verify the source of the IPv6 link-local address of a CPE.

Information About Cable DHCP Leasequery

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks begin scanning a range of IP addresses, in an attempt to find unused addresses. When the Cisco CMTS router is verifying unknown IP addresses, this type of scanning generates a large volume of DHCP leasequeries, which can result in the following problems:

- High CPU utilization on the Cisco CMTS router PRE card.
- High utilization on the DHCP servers, resulting in a slow response time or no response at all.
- Packets can be dropped by the Cisco CMTS router or DHCP server (or configured alternate server).
- Lack of available bandwidth for other customers on the cable interface.

To prevent such a large volume of leasequery requests on cable interfaces, you can enable filtering of these requests on upstream interfaces, downstream interfaces, or both. When the Cable DHCP Leasequery feature is enabled, the Cisco CMTS allows only a certain number of DHCP leasequery requests for each service ID

(SID) on an interface within the configured interval time period. If an SID generates more Leasequeries than the maximum, the router drops the excess number of requests until the next interval period begins.

You can configure both the number of allowable DHCP leasequery requests and the interval time period, so as to match the capabilities of your DHCP server (or configured alternate server) and cable network.

To configure the Cisco CMTS router to send DHCP leasequery requests to the DHCP server, use the **cable source-verify dhcp** and **no cable arp** commands. 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 returns a DHCP ACK message with the DHCP relay information and lease information of the CPE device that has been assigned this IP address, if any.

When **cable source-verify dhcp** and **no cable arp** commands are configured, DHCP leasequery is sent for downstream packets to verify unknown IP addresses within the IP address range configured on the cable bundle interface.

For DHCP leasequery to work in the downstream direction, the Cisco Network Registrar (CNR) should be made aware of the DHCP Option 82. This is required to make the CMTS map the CPE IP address to the correct CM. To do this, configure the **ip dhcp relay information option** command on the bundle interface to insert service class relay agent option into the DHCP DISCOVER messages. When the configuration is in place, during DHCP DISCOVER the values of DHCP Option 82 is cached by the CNR and is returned to the CMTS on any subsequent DHCP leasequery for that IP address.

To configure the Cisco CMTS router to divert DHCP leasequery requests to a server other than the DHCP server, use the **cable source-verify dhcp server ipaddress** and **no cable arp** commands.

The Cisco CMTS supports two types of DHCP leasequery implementation, Cisco standard compliant DHCP leasequery and RFC 4388 standard compliant DHCP leasequery. These two standards differ mostly in the identifiers used to query or respond to the DHCP Server. You can choose between these two implementations depending on which standard is supported on your DHCP Server.

Use the **ip dhcp compatibility lease-query client** {**cisco** | **standard**} command to configure the Cisco CMTS in either Cisco mode or RFC 4388 standard mode.

For more information about this command, see the "DHCP Commands" chapters in the *Cisco IOS IP Addressing Services Command Reference* , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html.

DHCP MAC Address Exclusion List

The Cisco IOS Release 12.3(13)BC introduces the ability to exclude trusted MAC addresses from the standard DHCP source verification checks, as supported in earlier 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 the Performance Routing Engine 1 (PRE1), PRE2, and PRE4 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP to pass without source verification checks, 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.

For more information on the cable trust command, see the Cisco IOS CMTS Cable Command Reference Guide .

Unitary DHCPv6 Leasequery

The Cisco IOS Release 12.2(33)SCF1 introduces support for unitary DHCPv6 leasequery protocol (RFC 5007) on the Cisco CMTS routers for upstream IPv6 source verification. This protocol verifies the authenticity of the IPv6 CPE behind a home or small office cable deployment.

If the IPv6 source verification fails on the router and the **cable ipv6 source-verify dhcp** and **no cable nd** commands are configured on the bundle interface or subinterface, the Cisco CMTS triggers a unitary DHCPv6 leasequery to the Cisco Network Registrar (CNR). If a valid leasequery response is received from the CNR, the Cisco CMTS adds the CPE to its subscriber database and allows future traffic for the CPE.

The primary use of the unitary DHCPv6 leasequery protocol on the Cisco CMTS router is to recover lost CPE data including the Prefix Delegation (PD) route. The IPv6 CPE data can be lost from the Cisco CMTS in several ways. For example, PD route loss can occur during a Cisco CMTS reload.

The unitary DHCPv6 leasequery protocol also supports the following:

- DHCPv6 leasequery protocol.
- Rogue client database for failed source-verify clients.
- DHCPv6 leasequery filters.
- DHCPv6 leasequeries to a specific DHCPv6 server.

How to Configure Filtering of Cable DHCP Leasequery Requests

Use the following procedures to configure the filtering of DHCP Leasequery requests on the Cisco CMTS downstreams and upstreams:

Enabling DHCP Leasequery Filtering on Downstreams

Use the following procedure to start filtering DHCP leasequeries on all downstreams of a cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable source-verify leasequery-filter downstream** *threshold interval* **Example:** `Router(config)# cable source-verify leasequery-filter downstream 5 10`	Enables leasequery filtering on all downstreams on the specified bundle interface, using the specified *threshold* and *interval* values.
Step 4	**end** **Example:** `Router(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Enabling DHCP Leasequery Filtering on Upstreams

Use the following procedure to start filtering DHCP Leasequeries on all upstreams on a bundle interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Enters interface configuration mode for the specified bundle interface.
Step 4	**cable source-verify leasequery-filter upstream** *threshold interval* **Example:** `Router(config-if)# cable source-verify`	Enables leasequery filtering on all upstreams on the specified bundle interface, using the specified *threshold* and *interval* values. **Note** The **cable source-verify leasequery-filter upstream** command can only be configured under bundle interface. **Note** Repeat step 3 and step 4 to enable the filtering of DHCP Leasequeries on the upstreams for other bundle interfaces. Master and slave interfaces in a cable bundle must be configured separately.

	Command or Action	Purpose
	`leasequery-filter upstream 2 5`	
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Unitary DHCPv6 Leasequery Filtering

Use the following procedure to configure the Cisco CMTS router to send Leasequeries to a DHCP server to verify the authenticity of the IPv6 CPE. You can also enable filtering of these requests to prevent large volumes of Leasequery requests on the bundle interfaces. Similarly, the number of allowable Leasequery requests and the interval time period can also be configured.

Note When the leasequery timer expires, only the IPv4 static CPE is automatically removed from the host database.

Before You Begin

- Disable the IPv6 Neighbor Discovery (ND) Gleaning feature using the **no** form of the **cable nd** command in bundle interface configuration mode before configuring the unitary DHCPv6 leasequery protocol. For details on IPv6 ND gleaning, see IPv6 on Cable feature guide.
- Configure the **cable ipv6 source-verify dhcp** command, introduced from Cisco IOS Release 12.2(33)SCF1 onwards, under the Cisco CMTS bundle or bundle subinterface to enable the unitary DHCPv6 leasequery protocol.
- In the cable ipv6 pd-route {enclosing-route | prefix-length} bundle-interface command, enclosing-route | prefix-length parameters should not be the same as IA_PD request and should be configured as a large prefix to include all the pd-route prefix for the downstream lease query.
- Use the **cable ipv6 source-verify dhcp** [**server** *ipv6-address]* command for a single DHCP server.
- *Use the* **cable ipv6 source-verify dhcp command without any keywords** *for multiple DHCP servers.*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Enters interface configuration mode for the specified bundle interface.
Step 4	**cable ipv6 source-verify** or**cable ipv6 source-verify dhcp** [server ipv6-address] **Example:** `Router(config-if)# cable ipv6 source-verify` `or` `Router(config-if)# cable ipv6 source-verify dhcp server 2001:DB8:1::1`	Enables leasequery filtering on the specified bundle interface and verifies the IP address with multiple DHCPv6 servers. or Enables leasequery filtering on the specified bundle interface and verifies the IP address with a specified DHCPv6 server.
Step 5	**cable ipv6 source-verify leasetimer** *value* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 200`	Enables leasequery timer on the specified bundle interface, for the Cisco CMTS to check its internal CPE database for IPv6 addresses whose lease time has expired.
Step 6	**cable ipv6 source-verify leasequery-filter** *threshold interval* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	Enables filtering of the IPv6 leasequery requests.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DHCPv6 Leasequery Filtering on Downstreams

Use the following procedure to start filtering DHCP Leasequeries on all downstreams of a cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable ipv6 source-verify leasequery-filter downstream** *threshold interval* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	Enables leasequery filtering on all downstreams on the specified bundle interface, using the specified threshold and interval values:
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Filtering of DHCP Leasequery

This section provides the following examples on how to configure the DHCP leasequery filtering feature:

Example: DHCP Leasequery Filtering

The following example shows an excerpt from a typical configuration of a bundle interface that is configured for filtering DHCP leasequery requests on both its upstream and downstream interfaces:

Note If an alternate server has been configured to receive leasequery requests, the **cable source-verify dhcp server** *ipaddress command* would display in place of the **cable source-verify dhcp** command below.

```
.
.
.
cable source-verify leasequery-filter downstream 5 20
```

```
.
.
.
interface bundle 1
.
.
.
 cable source-verify dhcp
 cable source-verify leasequery-filter upstream 1 5
 no cable arp
.
.
```

Example: Unitary DHCPv6 Leasequery Filtering

The following example shows how to display the total number of DHCPv6 leasequery requests that have been filtered on the router in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter
IPv4 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
IPv6 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
```

The following example shows how to display the total number of DHCP leasequery requests that have been filtered on a particular cable interface in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter cable 7/0/0

IPv4 Lease Query Filter statistics for Cable7/0/0:
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
IPv6 Lease Query Filter statistics for Cable7/0/0:
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
```

The following example shows how to display a list of cable modems on a cable interface and the number of DHCP leasequery messages filtered per interface in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter cable 7/0/0 requests-filtered

Sid  MAC Address    IP Address      Req-Filtered
1    0018.6835.2756 0.0.0.0         0
2    0025.2e2d.7440 0.0.0.0         0
Sid  MAC Address    IP Address          Req-Filtered
1    0018.6835.2756 2001:DB8:1::1       0
2    0025.2e2d.7440 2001:DB8:1::2       0
```

Troubleshooting

The following **debug** commands help you to troubleshoot an improper DHCPv6 leasequery filtering configuration:

- **debug cable ipv6—**Enables debug operation for the IPv6 transactions on a cable interface.
- **debug cable ipv6 db—**Displays debug messages associated with host database transactions.
- **debug cable ipv6 dhcp—**Displays debug messages associated with DHCPv6 transactions.
- **debug cable ipv6 ha—**Displays debug messages associated with High Availability (HA) IPv6 transactions.

- **debug cable ipv6 lq—**Displays debug messages associated with leasequery (LQ) transactions.
- **debug cable ipv6 nd—**Displays debug messages associated with Neighbor Discovery (ND) transactions.
- **debug cable ipv6 source-verify—**Displays debug messages associated with source verification transactions.

For detailed information on these and other debug commands, see the Cisco IOS CMTS Cable Command Reference Guide .

Additional References

The following sections provide references related to the Cable DHCP Leasequery feature.

Related Documents

Related Topic	Document Title
IPv6	IPv6 on Cable
Cisco CMTS Command Reference	Cisco IOS CMTS Cable Command Reference Guide
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/security/command/ reference/fsecur_r.html

Standards

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	*An Ethernet Address Resolution Protocol (ARP)*
RFC 4388	Dynamic Host Configuration Protocol (DHCP) Leasequery
RFC 5007	Unitary DHCPv6 Leasequery

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable DHCP Leasequery

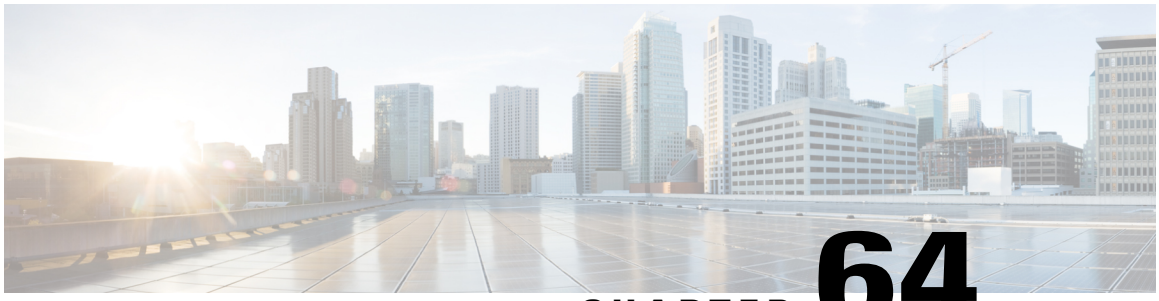
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 180: Feature Information for Cable DHCP Leasequery

Feature Name	Releases	Feature Information
Cable DHCP Leasequery	12.2(15)BC1d, 12.2(15)BC2b	This feature was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers.

Feature Name	Releases	Feature Information
Cable DHCP Leasequery	12.3(13)BC	Added support for the MAC Address Exclusion List for the cable-source verify dhcp command.
Filtering Cable DHCP Leasequery	12.3(17a)BC	Added support for the configurable leasequery server using the cable source-verify dhcp server ipaddress command.
RFC4388 Compliance Cable Leasequery	12.2(33)SCE1	Added support for RFC 4388 compliant DHCP leasequery. The **ip dhcp compatibility lease-query client** {**cisco** | **standard**} command was integrated to this feature.
Unitary DHCPv6 Leasequery protocol (RFC 5007)	12.2(33)SCF1	Added support for RFC 5007 compliant DHCPv6 leasequery protocol. The following sections provide information about this feature: The following commands were introduced or modified: **cable ipv6 source-verify, cable ipv6 source-verify leasequery-filter downstream, show cable leasequery-filter**, and **debug cable ipv6 lq**.



CHAPTER 64

Service Independent Intercept on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 11, 2012

In Cisco IOS Release 12.2(33)SCA, the Service Independent Intercept (SII) feature enhances the current Lawful Intercept (LI) capability for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers using SNMPv3.

In releases prior to Cisco IOS Release 12.2(33)SCA, the Cisco cable modem termination system (CMTS) routers supported these LI capabilities:

- Intercepts for voice traffic in PacketCable environments
- IPv4 intercepts for SII using SNMPv3
- CLI for MAC intercepts

SII extends these LI capabilities in Cisco IOS Release 12.2(33)SCA and later releases by adding support for customer premise equipment (CPE) and cable modem (CM) based MAC intercepts using SNMPv3. SII is designed to provide data intercepts through SNMPv3, while PacketCable intercepts are designed for VoIP intercepts using a Common Open Policy Service (COPS) interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Service Independent Intercept

Before configuring SII, an understanding of the SNMPv3 configuration is required. Ensure that SNMPv3 is configured on the router.

Note SII intercepts are supported only on cable bundle interfaces.

This table shows the hardware compatibility prerequisites for this feature.

Table 181: Service Independent Intercept on the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2[129] Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [130]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [131]

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

129 PRE = Performance Routing Engine

130 Cisco uBR-MC3GX60V cable interface line card is compatible only with PRE4.

131 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2

Restrictions for Service Independent Intercept

- IPv6 addressing for IP intercepts is supported on the Cisco uBR10012 router from Cisco IOS Release 12.2(33)SCG onwards.
- Mediation device (MD) must be reachable through the global IP routing table. Support for an MD inside an Multiprotocol Label Switching (MPLS)/VPN is not supported.
- SII information cannot be displayed using CLI. Intercept content from SII will not appear in the **show pxf cable** commands. Other intercept information outside of SII content (for PacketCable and through the CLI intercept) is shown.
- Cisco uBR10012 router has the following MIB object restrictions:
  - When a PRE switchover occurs, the SII configuration is lost. An SNMP trap is generated for this event. The SII must be configured after a PRE switchover.
  - cTap2MediationDestAddressType—IPv6 is not supported.
  - cTapMediationRtcpPort—Not supported.
  - cTapMediationRetransmitType—Not supported.
  - cTapMediationTransport—UDP only.
  - cTapStreamIpInterface—Only if interface supported is cable.
  - cTapStreamIpAddrType—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.
  - cTapStreamIpDestinationLength—Must be 32 (no subnets are supported) or 0. The address length and port range restrictions are only for IPv4. There is no restriction for IPv6.
  - cTapStreamIpFlowId—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.
  - cTapStreamIpDestL4PortMin—Must match DestL4PortMax or have a value of 0.

- cTapStreamIpDestL4PortMax—Must match DestL4PortMin or have a value of 65535.
- cTapStreamIpSourceL4PortMin—Must match SourceL4PortMin or have a value of 0.
- cTapStreamIpSourceL4PortMax—Must match SourceL4PortMax or have a value of 65535.

- Maximum number of IP intercepts allowed is 800.
- Maximum number of MAC intercepts allowed is 400.

Note Performance is measured based on the total bit rate and bandwidth based on the tapped traffic rather than the stream number. For example, one MAC intercept may carry 300 Mbps of traffic while a normal VoIP traffic may be around 80 Kbps.

Information About Service Independent Intercept

SII has the following benefits:

- Does not affect subscriber services on the router.
- Can neither be detected by the target, nor tapped.
- Allows Law Enforcement Agencies (LEAs) to perform lawful intercepts without the knowledge of service providers.
- Uses Simple Network Management Protocol version 3 (SNMPv3) and security features like the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- Supports intercepts of Layer 2, Layer 3, and Layer 4 traffic.
- Supports Layer 2 intercepts for upstream and downstream traffic.
- Hides information about lawful intercepts from all but the most privileged users.
- Provides two secure interfaces for performing an intercept—one for setting up the wiretap and one for sending the intercepted traffic to the MD.
- Coexists with Packet Intercept (PI). To support PI in a PacketCable environment for voice intercepts, you must enable PacketCable operation must be enabled on the Cisco CMTS and other related PacketCable configurations must be implemented as required. For more information about PacketCable and lawful intercept, see the PacketCable and PacketCable Multimedia for the Cisco CMTS Routers and Lawful Intercept Architecture feature guides.

Before configuring SII on the Cisco CMTS, understand the following concepts:

Lawful Intercept

LI is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (also known as target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require SPs and ISPs to implement their networks to explicitly support authorized electronic surveillance.

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks. The LEA delivers a request for a wiretap to the service provider of the target, who is responsible for intercepting data communication to and from the target. The service provider uses the MAC address or session ID of the target to determine which of its edge routers handles the traffic (data communication) of the target. The service provider then intercepts the traffic of the target as it passes through the router, and sends a copy of the intercepted traffic to the LEA without the knowledge of the target.

The LI feature supports the Communications Assistance for Law Enforcement Act (CALEA), which specifies that SP in the United States must support lawful intercept. Currently, LI is defined by the following standards:

- Telephone Industry Association (TIA) specification J-STD-025
- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

Packet Intercept

PI describes a Cisco CMTS-specific implementation for lawful intercept on Cisco CMTS routers. PI is supported through two interfaces. In a PacketCable environment, PI provides voice intercept capability for IP intercepts using COPS to support CALEA. Using a CLI interface (**cable intercept** command), PI also supports MAC intercepts.

For more information about PacketCable Lawful Intercept, PacketCable configuration on the Cisco CMTS, and COPS support on the Cisco CMTS, see the PacketCable and PacketCable Multimedia for the Cisco CMTS Routers .

Service Independent Intercept

SII describes a standard Cisco architecture (RFC 3924, Cisco Architecture for Lawful Intercept in IP Networks) that provides Layer 1 capabilities using an SNMPv3 interface.

SII supports a different intercept method than PI on the Cisco CMTS router by using SNMPv3 for both MAC and IP intercepts. Although SII is a distinct method from PI, SII can coexist with PI-based intercepts in Cisco IOS Release 12.2(33)SCA and later releases.

Service Independent Intercept Tap in Routed Subnets

In Cisco IOS Release 12.2(33)SCE and earlier releases, it is assumed that the “IP tap” on the Cisco CMTS cable interface is a legal IP address acquired from the Cisco Network Registrar (CNR), which can pass reverse path forwarding (RPF) verification. Based on this assumption, a tapped IP address is defined under the scope of the cable bundle interface subnet, such as:

```
ip address <ip-address> <subnet-mask> or ip address <ip-address> <subnet-mask> secondary
```

For example: ip address 80.32.0.1 255.255.255.0

Cisco IOS Release 12.2(33)SCF and later releases do not have any CNR restrictions.

The source IP address or the destination IP address of a tapped stream is normally learned from a routing protocol or provisioned by a static route. When a CPE acts as a router, the IP route behind the CPE is not allocated by the CNR DHCP. Therefore, the destination IP address is not defined in the bundle interface subnet.

Starting with Cisco IOS Release 12.2(33)SCF, the SII provisioning mode is supported in the route processor and on the Cisco IOS LI.

For more information, see the Provisioning Taps on IP addresses Learned from the CPE Router, on page 1714.

IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept feature provides lawful intercept of cable modems and CPEs provisioned with IPv6 addresses. This feature taps all the packets received and sent from the system. The intercepted packets are sent to the MD with the content connection identifier (CCCID) specified by the tapping rule.

The following types of IPv6 taps are supported on the Cisco CMTS router:

- IPv6 Taps—Matches all IPv6 packets.
- 6PE Taps—Supports IPv6 Provider Edge (6PE) deaggregation. However, disposition packets are not supported.
- 6VPE Taps—Matches all IPv6 packets in the virtual routing and forwarding (VRF) context. Disposition packets are not supported.

The IPv6 Address Packet Intercept feature provides these benefits on a Cisco CMTS router:

- Supports up to 1000 IPv6 taps.
- Supports IPv4 and MAC taps.
- Supports up to 4000 mediation devices.
- Intercepts and forwards up to 100,000 packets per second.

In the Cisco CMTS, IPv6 taps can be applied only to the cable interfaces. However, the Cisco CMTS can search for the interface using the IPv6 routing table using the IPv6 source (src) and destination (dst) address tap. A tap request on the cable interface will fail only if the tap requests exceed the maximum number of taps supported on the Cisco CMTS.

A forwarding packet can be tapped at both the input and output interface, and a single packet may be hit by more than one tapping rule. However, the Cisco CMTS will send only one replication of the forwarding packet to the MD. Likewise, both IPv6 address taps and MAC taps can be provisioned. If the packet matches both the taps, the MAC tap will take priority and the packet will be sent only to the MD of the MAC tap.

MPLS and VPN Support

The IPv6 Address Packet Intercept supports MPLS and VPN at the Provider Edge (PE) router. The VRF processes the MPLS and VPN traffic, and interception is performed on the IPv6 packet under VRF.

Compatibility with Other Taps

The SII Access Control List (ACL) tap is compatible with other kinds of tap, such as MAC tapping, CALEA, and hash table based IPv4 tapping. It also coexists with security ACL, quality of service (QoS) ACL, cable filter, overlapping tap, and multiple MDs. However, SII ACL tap will not work with Layer 2 VPN (L2VPN) and Any Transport Over MPLS (AToM) packets.

Network Components Used for Lawful Intercept

Mediation Device

A mediation device (supplied by third-party vendor) handles most of the processing for the lawful intercept. The mediation device:

- Provides the interface used to set up and provision the lawful intercept.
- Generates requests to other network devices to set up and run the lawful intercept.
- Converts the intercepted traffic into the format required by the LEA (which can vary from country to country) and sends a copy of the traffic to the LEA without the knowledge of the target.

Note If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA. The mediation device is also responsible for restarting any lawful intercepts that are disrupted due to a failure.

Intercept Access Point

An intercept access point (IAP) is a device that provides information for the lawful intercept. There are two types of IAPs:

- Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept related information (IRI) for the intercept (for example, the username of the target and system IP address). The IRI helps the service provider determine which content IAP (router) the traffic of the target passes through.
- Content IAP—A device, such as a Cisco CMTS router, through which the traffic of the target passes through. The content IAP:
  - Intercepts traffic to and from the target for the length of time specified in the court order. The router continues to forward traffic to its destination to ensure that the wiretap is undetected.
  - Creates a copy of the intercepted traffic, encapsulates it in UDP packets, and forwards the packets to the mediation device without the knowledge of the target.

Note The content IAP sends a single copy of intercepted traffic to the mediation device. If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA.

Collection Function

The collection function is a program that stores and processes traffic intercepted by the service provider. The program runs on the equipment at the LEA.

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the service provider of the target. The service provider determines the appropriate router to set up the tap and forwards the intercepted packets to the mediation device, which might be located outside of the premises of the service provider.

There is no standard method in a PacketCable environment for setting up a tap for voice traffic. SII provides a standard way for setting up data taps by either an IP or MAC address. SII includes two ways of setting a MAC-based tap:

- On CPE—Only intercepts traffic whose source or destination match the MAC address of the CPE device.
- On CM—Intercepts all of the traffic behind the CM, including the CM traffic itself. This form of intercept might generate a lot of traffic to the mediation device.

The following sequence of events provides an example of a process that might be used during a sample lawful intercept:

- The admin function at the service provider contacts the ID IAP for the IRI, such as the username of the target and the IP address of their system, to determine which content IAP (router) the traffic of the target passes through.
- After identifying the router that handles the traffic of the target, the admin function issues SNMPv3 **get** and **set** requests to the router MIBs to set up and activates the lawful intercept. The router MIBs include the CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, and CISCO-802-TAP-MIB.
- During the lawful intercept, the router:
  - Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
  - Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.
  - Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the knowledge of the target.

Note The process of intercepting and duplicating the traffic of the target adds no detectable latency in the traffic stream.

- The mediation device converts the intercepted traffic into the required format and sends it to a collection function running at the LEA. Here, the intercepted traffic is stored and processed.

Note If the router intercepts traffic that is not allowed by the judicial order, the mediation device filters out the excess traffic and sends the LEA only the traffic allowed by the judicial order.

- When the lawful intercept expires, the router stops intercepting the traffic of the target.

SNMPv3 Interface

SII supports the following MIBs in SNMPv3:

- CISCO-TAP2-MIB, on page 1703
- CISCO-IP-TAP-MIB, on page 1704
- CISCO-802-TAP-MIB, on page 1706

For more information on the Cisco IOS MIB tools, see the the MIB Locator page.

CISCO-TAP2-MIB

The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts on the router. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the router. The MIB is bundled with Cisco IOS software images that support the Service Independent Intercept feature.

The CISCO-TAP2-MIB works with the CISCO-IP-TAP-MIB and the CISCO-802-TAP-MIB to define specific intercepts.

Table 182: CISCO-TAP2-MIB Tables and Objects

Object	Description
cTap2MediationTable	Lists the MDs with which the intercepting device communicates.
cTap2StreamTable	Lists the traffic streams to be intercepted. Consists of generic fields that are independent of the type of intercept.
cTap2DebugTable	Contains LIt debug messages generated by the implementing device.
cTap2MediationNewIndex	Contains a value which may be used as an index value for a new cTap2Mediation object entry.
cTap2MediationCapabilities	Displays the device capabilities for certain fields in the MD. This may be dependent on hardware or software capabilities.
cTap2DebugAge	Contains the duration in minutes for which an entry in the cTap2DebugTable object is maintained by the implementing device. The entry is deleted when this duration is reached.
cTap2DebugMaxEntries	Contains the maximum number of debug messages maintained at one time by the implementing device. When this limit is reached, the most recent message replaces the oldest message.

Table 183: CISCO-TAP2-MIB Notifications , on page 1704 lists the notifications in the CISCO-TAP2-MIB. For more information, see the MIB documentation.

Table 183: CISCO-TAP2-MIB Notifications

Notification	Description
ciscoTap2MIBActive	Sent when an intercepting router or switch is first capable of intercepting a packet corresponding to a configured data stream. The value of the corresponding cTap2StreamType object that identifies the actual intercept stream type is included in this notification.
ciscoTap2MediationTimedOut	Sent when an intercept is autonomously removed by an intercepting device, such as due to the time specified in the cTap2MediationTimeout object.
ciscoTap2MediationDebug	Sent when there is intervention needed due to events related to entries configured in the cTap2MediationTable object.
ciscoTap2StreamDebug	Sent when there is intervention needed due to events related to entries in the cTap2StreamTable object.
ciscoTap2Switchover	Sent when there is a redundant (standby) route processor available on the intercepting device and the current active processor is going down causing the standby to takeover.

CISCO-IP-TAP-MIB

The CISCO-IP-TAP-MIB contains the SNMP management objects to configure and execute lawful intercepts on IP Layer 3 streams. This MIB is used with the CISCO-TAP2-MIB to intercept traffic based on the IP address.

Note The Cisco CMTS routers supports IPv6 IP intercepts only from Cisco IOS Release 12.2(33)SCG onwards.

Table 184: CISCO-IP-TAP-MIB Tables and Objects

Object	Description
citapStreamTable	Lists the IP streams to be intercepted.
citapStreamCapabilities	Displays the type of intercept streams that can be configured on this type of device.

Object	Description
citapStreamInterface	Lists the ifIndex value of the interface over which the traffic to be intercepted is received or transmitted.
citapStreamAddrType	Lists the type of address used in the packet selection.
citapStreamDestinationAddress	Lists the destination address or prefix used in the packet selection. This address is of “type” specified in the citapStreamAddrType.
citapStreamDestinationLength	Lists the length of the destination prefix. A value of zero causes all addresses to match.
citapStreamSourceAddress	Lists the source address used in the packet selection. This address is of “type” specified in the citapStreamAddrType object.
citapStreamSourceLength	Lists the length of the source prefix. A value of zero causes all addresses to match. This prefix length is consistent with the “type” specified in the citapStreamAddrType object.
citapStreamTosByte	Lists the value of the ToS byte when masked with citapStreamTosByteMask object, of traffic to be intercepted. If citapStreamTosByte&(~citapStreamTosByteMask)!=0, the configuration is rejected.
citapStreamTosByteMask	Lists the value of the ToS byte in an IPv4 header. The AND operation is performed on the citapStreamTosByteMask and citapStreamTosByte objects; if the values are equal, the comparison is equal. If the mask is zero and the ToS byte value is zero, the result is to always accept.
citapStreamFlowId	Lists the flow identifier in an IPv6 header. -1 indicates that the flow ID is unused.
citapStreamProtocol	Lists the IP protocol that must be matched against the IPv4 protocol number in the packet. -1 means “any IP protocol”.
citapStreamDestL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or less than the value specified for this entry in the citapStreamDestL4PortMax object.

Object	Description
citapStreamDestL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamDestL4PortMin object.
citapStreamSourceL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match. This value must be equal to or less than the value specified for this entry in the citapStreamSourceL4PortMax object.
citapStreamSourceL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamSourceL4PortMin object.
citapStreamVRF	Lists the name of a VRF table (ASCII string) comprising the routing context of a VPN. The interface or set of interfaces on which the packet may be found should be selected from the set of interfaces in the VRF table. A string length of zero implies that the global routing table must be used for selection of interfaces on which the packet might be found.

CISCO-802-TAP-MIB

The CISCO-802-TAP-MIB contains the SNMP management objects to configure and execute lawful intercepts on Layer 2 streams. This MIB is used with the CISCO-TAP2-MIB to intercept traffic based on the MAC address.

The Cisco CMTS routers in Cisco IOS Release 12.2(33)SCA support MAC-based intercepts for both the cable modem (CM) and the CPE using SNMPv3.

Table 185: CISCO-802-TAP-MIB Tables and Objects

Object	Description
c802tapStreamTable	Lists the IEEE 802 data streams to be intercepted.
c802tapStreamCapabilities	Displays the types of intercept streams that can be configured on this device. This may be dependent on hardware or software capabilities.
citapStreamInterface	Lists the ifIndex value of the interface over which the traffic to be intercepted is received or transmitted.

Object	Description
citapStreamAddrType	Lists the type of address used in the packet selection.
citapStreamDestinationAddress	Lists the destination address or prefix used in the packet selection. This address is of "type" specified in the citapStreamAddrType object.
citapStreamDestinationLength	Lists the length of the destination prefix. A value of zero causes all addresses to match.
citapStreamSourceAddress	Lists the source address used in the packet selection. This address is of "type" specified in the citapStreamAddrType object.
citapStreamSourceLength	Lists the length of the source prefix. A value of zero causes all addresses to match. This prefix length is consistent with the "type" specified in the citapStreamAddrType object.
citapStreamTosByte	Lists the value of the ToS byte when masked with the citapStreamTosByteMask object, of traffic to be intercepted. If citapStreamTosByte&(~citapStreamTosByteMask)!=0, the configuration is rejected.
citapStreamTosByteMask	Lists the value of the ToS byte in an IPv4 header. The AND operation is performed on the citapStreamTosByteMask and citapStreamTosByte objects; if the values are equal, the comparison is equal. If the mask is zero and the ToS byte value is zero, the result is to always accept.
citapStreamFlowId	Lists the flow identifier in an IPv6 header. -1 indicates that the flow ID is unused.
citapStreamProtocol	Lists the IP protocol that must be matched against the IPv4 protocol number in the packet. -1 means "any IP protocol".
citapStreamDestL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match. This value must be equal to or less than the value specified for this entry in the citapStreamDestL4PortMax object.
citapStreamDestL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamDestL4PortMin object.

Object	Description
citapStreamSourceL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or less than the value specified for this entry in the citapStreamSourceL4PortMax object.
citapStreamSourceL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamSourceL4PortMin object.
citapStreamVRF	Lists the name of a VRF table (ASCII string) comprising the routing context of a VPN. The interface or set of interfaces on which the packet may be found should be selected from the set of interfaces in the VRF table. A string length of zero implies that the global routing table must be used for selection of interfaces on which the packet might be found.

How to Perform SNMPv3 Provisioning for Service Independent Intercept

This section includes the following procedures:

Prerequisites for SNMPv3 Provisioning

- Ensure you are logged in to the router with the highest access level (level-15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.
- Ensure that the mediation device has an access function (AF) and an access function provisioning interface (AFPI).
- Ensure that you have added the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view, using the **snmp-server user** command. Specify the username of the mediation device as the user to add to the group.
- Ensure that when you add the mediation device as a CISCO-TAP2-MIB user, the authorization password of the mediation device must be at least eight characters in length.

Restrictions to SNMPv3 Provisioning

- The only users who should be allowed to access the Lawful Intercept MIBs are the mediation device and system administrators who need to know about lawful intercepts on the router. In addition, these users must have authPriv or authNoPriv access rights to access the SII MIBs. Users with NoAuthNoPriv access cannot access the Lawful Intercept MIBs.

- You cannot use the SNMP-VACM-MIB to create a view that includes the Lawful Intercept MIBs.
- The default SNMP view excludes the following MIBs:
  - CISCO-TAP2-MIB
  - CISCO-IP-TAP-MIB
  - SNMP-COMMUNITY-MIB
  - SNMP-USM-MIB
  - SNMP-VACM-MIB
- The Cisco CMTS router does not display log messages about SII taps; therefore, you can only see configuration errors by using SNMP traps.
- The Cisco CMTS router does not display any details about SII taps in **show pxf cable** commands. A line in the output of the **show pxf cable** command displays the number of SII taps, but not their content.
- The Cisco CMTS router supports IPv6 addressing for IP taps only from Cisco IOS Release 12.2(33)SCG onwards.

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs supported by SII are only available in software images that support the SII and Lawful Intercept features. These MIBs are not accessible through the Network Management Software MIBs Support page.

In Cisco IOS Release 12.2(33)SCA and later releases, the Cisco CMTS routers support LI and SII MIBs using the following images:

- Cisco uBR7246VXR router—ubr7200-k9pu2-mz
- Cisco uBR10012 router—ubr10k2-k9p6u2-mz

In Cisco IOS Releases 12.2(33)SCF and later releases, the Cisco CMTS routers support LI and SII MIBs using the following images:

- Cisco uBR10012 router with PRE2—ubr10k2-k9p6u2-mz
- Cisco uBR10012 router with PRE4—ubr10k4-k9p6u2-mz
- Cisco uBR7246VXR router with NPE-G1—ubr7200-ik9su2-mz
- Cisco uBR7246VXR router with NPE-G2—ubr7200p-jk9su2-mz

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about LI should be allowed to access the LI MIBs. To restrict access to these MIBs, you must complete the following tasks:

- Create a view that includes the Cisco LI MIBs.
- Create an SNMP user group that has read and write access to the view. Only users assigned to this user group can access information in the MIBs.

- Add users to the Cisco LI user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view***view-name oid-tree* **included** **Example:** `Router(config)# snmp-server view tapView ciscoIpTapMIB included`	Creates or updates a view entry. • **view** *view-name*—Label for the view record that you are updating or creating. The name is used to reference the record. • *oid-tree*—Object identifier of the ASN.1 subtree. • **included**—Type of view. Repeat this step as needed to include other MIBs in the view.
Step 4	**snmp-server group***groupname* **v3 noauth read***readview* **write***writeview* **notify***notifyview* **Example:** `Router(config)# snmp-server group tapGroup v3 noauth read tapView write tapView notify tapView`	Configures a new SNMPv3 group. • *groupname*—SNMP server group name. • **v3**—The most secure of the possible security models. • **noauth**—Specifies no authentication of a packet. • **read**—The option that allows you to specify a read view. • *readview*—A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent. • **write**—The option that allows you to specify a write view. • *writeview*—A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent. • **notify**—The option that allows you to specify a notify view.

	Command or Action	Purpose
		• *notifyview*—A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
Step 5	**snmp-server user** *username groupname* **v3 auth md5** *auth-password* **Example:** `Router(config)# snmp-server user tapuser tapGroup v3 auth md5 cisco`	Configures a new user to an SNMPv3 group • *username*—The name of the user on the host that connects to the agent. • *groupname*—The name of the group to which the user is associated. • **v3**—The most secure of the possible security models. • **auth**—Initiates an authentication level setting session • **md5**—The HMAC-MD5-96 authentication level. • *auth-password*—A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying the SNMP Configuration

Use the following commands to verify the configuration of SNMP:

Command	Description
show snmp group	Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group.
show snmp user	Displays information about the configured characteristics of SNMP users.
show snmp view	Displays the family name, storage type, and status of an SNMP configuration and associated MIB.

Provisioning the Cable Interface Using SNMPv3

1. Establish the mediation device first.
2. Provision the cable interface for which intercepts should be enabled by configuring objects in both the CISCO-802-TAP-MIB and the CISCO-IP-TAP-MIB:
   - CISCO-802-TAP-MIB—Configure the c802tapStreamInterface object.
   - CISCO-IP-TAP-MIB—Configure the citapStreamInterface object.
3. Use the c802tapStreamInterface and citapStreamInterface objects to specify the ifIndex of the desired interface. Use a -1, 0, or the address of the cable bundle interface.

Provisioning IP Intercepts Using SNMPv3

1. Configure objects in the CISCO-TAP2-MIB:

Configure the cTap2StreamEntry table object with the cTap2StreamType object configured for IP. This entry is used with the citapStreamEntry table object in the CISCO-IP-TAP-MIB.

1. Configure objects in the CISCO-IP-TAP-MIB:

Configure the ciTapStreamEntry table object that provides the details of the intercept in the CISCO-IP-TAP-MIB. This entry is used with the cTap2StreamEntry table object in the CISCO-TAP2-MIB.

1. Set the cTap2StreamInterceptEnable object bit.

Note IP intercepts also have interface OIDs. For more information, see the Provisioning the Cable Interface Using SNMPv3, on page 1712.

Provisioning IPv6 Taps Using SNMPv3

The IPv6 Address Packet Intercept is provisioned through SNMPv3. The MIBs involved in configuring IPv6 address tap are CISCO-IP-TAP-MIB and CISCO-TAP2-MIB. CISCO-IP-TAP-MIB object ID (OID) specifies the IPv6 packet stream. CISCO-TAP2-MIB OID specifies the MD, as to where and how to send the intercepted packet.

The IPv6 tap request should comply with the CISCO-IP-TAP-MIB and CISCO-TAP2-MIB to provision tap. The Cisco CMTS accepts each tap rule provisioned through SNMPv3 and sends the intercepted packet to the MD with the CCCID specified by the tapping rule.

The basic difference of IPv6 address tap from IPv4 address tap is that you have to specify the IPv6 address type and assign IPv6 address at the source and destination fields. Except the flow identifier, which is not used in IPv4 tap, all the other OIDs used by the IPv6 address tap are the same as of IPv4 address tap.

Restrictions for IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept has the following specific restrictions in addition to the general IPv4 address tapping restrictions.

- The IPv6 address tap through SNMP MIB is supported only on the Cisco uBR10012 series routers.
- The IPv6 address tap provision is not supported on the Cisco uBR7200 series routers. Any SNMP request on these routers will fail.
- The IPv6 packet intercept can be performed at the Cisco uBR7200 series routers only by setting up the MAC tap.
- The Cisco CMTS router does not support IPv6 multicast address tap on cable interfaces.
- The Cisco CMTS router supports only IPv4 MD encapsulation.
- The MPLS/VPN supports imposition and deaggregation.
- The IPv4 or IPv6 packets within an L2VPN or AToM will not be tapped.
- The IPv6 taps are supported only on cable interfaces.
- The IPv6 packet will be tapped only once.
- The IPv6 packets that come in as fragments without L4 fields are intercepted.

To provision the cable interface using SNMPv3, see Provisioning the Cable Interface Using SNMPv3, on page 1712.

The IPv6 packet can also be tapped per CPE and per CM MAC address. For more details, see the Provisioning MAC Intercepts Using SNMPv3, on page 1713.

Provisioning MAC Intercepts Using SNMPv3

SII in Cisco IOS Release 12.2(33)SCA on the Cisco CMTS routers allows you to provision bidirectional MAC intercepts (supports the upstream and downstream path) for a CM or CPE using SNMPv3.

The cmMacAddress object is used to specify the MAC address of either the CPE device or CM, and therefore is the object that determines the type of MAC intercept used.

Prerequisites for Provisioning MAC Intercepts using SNMPv3

- The CM must be online before the MAC intercept can be configured using SNMPv3.
- Set the CM bit only if you want to configure a CM-based tap.
- The destination (dstMACAddress) and source MAC address (srcMacAddress) bits must both be set.
- The values of the destination (c802tapStreamDestinationAddress) and source address (c802tapStreamSourceAddress) objects must have identical values.

Note If both destination and source MAC bits are not set, or the MAC address values do not match, the tap is rejected.

Restrictions to Provisioning MAC Intercepts using SNMPv3

- SII interface taps are only supported on cable line card bundle interfaces.

You can provision the following MAC intercepts using SNMPv3:

- Provisioning a MAC Intercept for Cable Modems Using SNMPv3, on page 1714
- Provisioning a MAC Intercept for a CPE Device Using SNMPv3, on page 1714
- Provisioning Taps on IP addresses Learned from the CPE Router, on page 1714

Provisioning a MAC Intercept for Cable Modems Using SNMPv3

1. Configure the c802tapStreamInterface object.
2. Set the following bit flags in the c802tapStreamFields object:
   - dstMacAddress (bit 1)
   - srcMacAddress (bit 2)
   - cmMacAddress (bit 6)—The cmMacAddress bit field is newly introduced for cable modem support and determines whether the intercept is a CPE-based or CM-based intercept.
3. Configure the following objects with the same CM MAC address value:
   - c802tapStreamDestinationAddress
   - c802tapStreamSourceAddress

Provisioning a MAC Intercept for a CPE Device Using SNMPv3

1. Configure the c802tapStreamInterface object.
2. Set the following bit flags in the c802tapStreamFields object:
   - dstMacAddress (bit 1)
   - srcMacAddress (bit 2)
3. Configure the following objects with the same CPE MAC address value:
   - c802tapStreamDestinationAddress
   - c802tapStreamSourceAddress

Provisioning Taps on IP addresses Learned from the CPE Router

Note To provision taps, the IP address must be available to the Cisco CMTS either through a routing protocol or by specifying the interface for the tap.

When a routed CPE is provisioned, the Cisco CMTS checks if the CPE is reachable by using the routing table. The Cisco CMTS can learn the route in the routing table through routing protocols, such as:

- Routing Information Protocol (RIP)
- RIP2

- Static route

The route can also be manually configured on the Cisco CMTS (static route).

Static route can be manually added by executing the **ip route** *destination netmask next-hop* command. For example, ip route 192.168.80.0 255.255.255.0 172.27.184.69 .

Use the **show ip route** command to verify if the static route has been configured. The routing protocol can also be viewed by running the **show ip route** command.

Note Starting with Cisco IOS Release 12.2(33)SCF, SII taps can be configured to an IP address learned from a CPE router.

Table 186: IP Address Tap , on page 1715 and Table 187: MAC Address Tap , on page 1716 display the conditions when a tap is successful.

Table 186: IP Address Tap

Source IP[132]	Destination IP	Specified Interface (bundle interface)	IP Subnet – Statically Configured or Learned on any Cable Interface	IP Subnet – Statically Configured or Learned on a Specified Cable Interface	Tap Enable?	Tap Success?
Yes	Yes	No	Yes	—[133]	Yes	Yes
Yes	Wildcard[134]	No	Yes	—	Yes	Yes
Wildcard	Yes	No	Yes	—	Yes	Yes
Wildcard	Wildcard	No	—	—	—	No
Yes	Yes	Yes	X	Yes	Yes	Yes
Yes	Wildcard	Yes	X	Yes	Yes	Yes
Wildcard	Yes	Yes	X	Yes	Yes	Yes
Wildcard	Wildcard	Yes	—	—	—	No
X[135]	X	X	No	No	—	No

132 Source IP, Destination IP, and Specified Interface columns are the OIDs from the SNMP.

133 "—" indicates that the item is not available or not applicable.

134 Wildcard is a subnet mask of 0.0.0.0

135 "X" can indicate either Yes or No.

Note The IP address presented at the Cisco CMTS Cable interface, Tap Enable, and Tap Success columns refer to the state on the Cisco CMTS.

Table 187: MAC Address Tap

Source MAC Address	Destination MAC Address	Specified Interface (Cable Interface)	MAC Address Presented at the Cisco CMTS Cable Interface	MAC Address Presented at the Specified Cable Interface	Tap Enable	Tap Success?
Yes	Yes	No	Yes	—[136]	Yes	Yes
Yes	Wildcard[137]	No	Yes	—	—	No*[138]
Wildcard	Yes	No	Yes	—	—	No*
Wildcard	Wildcard	No	—	—	—	No*
Yes	Yes	Yes	X	Yes	Yes	Yes
Yes	Wildcard	Yes	X	Yes	—	No*
Wildcard	Yes	Yes	X	Yes	—	No*
Wildcard	Wildcard	Yes	—	—	—	No
Yes	Yes	X	No	No	No**[139]	Yes**
Yes	Wildcard	X	X	X	—	No*
Wildcard	Yes	X	X	X	—	No*
X[140]	X	X	No	No	—	No

136 "—" indicates that the item is not available or not applicable.

137 Wildcard is a subnet mask of 0.0.0.0.

138 Both the source and destination MAC addresses must be present.

139 This is a preconfiguration case indicating that the CPE or the CM is not online.

140 "X" can indicate either Yes or No.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. This is because the default value of the cTap2MediationNotificationEnable object is true(1).

The **snmp-server enable traps snmp** command configures the router to send RFC 1157 notifications to the mediation device.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *hostname* **version3noauth** *community-string* **udp-port** *port notification-type* **Example:** `Router(config)# snmp-server host 10.10.10.10 version 3 noauth mdpass udp-port 161 snmp`	Specifies the recipient of an SNMP notification operation. • *hostname*—Name or Internet address of the host (the targeted recipient). • **version3**—Version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the priv keyword. If you use the version keyword, you should also specify a security level. • **noauth**—The noAuthNoPriv security level. This is the default value. • *community-string*—Password-like community string sent with the notification operation. • **udp-port**—UDP port of the host to use. The default is 162. • *notification-type*—Type of notification to be sent to the host. If no type is specified, all notifications are sent.
Step 4	**snmp-server enable traps snmp** [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**] **Example:** `Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	Enables the sending of RFC 1157 SNMP notifications. • **authentication**—(Optional) Controls the sending of SNMP authentication failure notifications. • **linkup**—(Optional) Controls the sending of SNMP linkUp notifications. • **linkdown**—(Optional) Controls the sending of SNMP linkDown notifications.

	Command or Action	Purpose
		• **coldstart—**(Optional) Controls the sending of SNMP coldStart notifications. • **warmstart—**(Optional) Controls the sending of SNMP warmStart notifications.
Step 5	**snmp-server enable traps** [*notification-type*] [**vrrp**] **Example:** `Router(config)# snmp-server enable traps tty`	Enables all SNMP notification types that are available on your system. • *notification-type***—**(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). • **vrrp—**(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Disabling SNMP Notifications

- To disable all SNMP notifications, use the **no snmp-server enable traps** command.
- To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To re-enable lawful intercept notifications through SNMPv3, reset the object to true(1).

Configuration Examples for SNMPv3 Provisioning for Service Independent Intercept

```
Router# show running-config | include snmp
snmp-server engineID local 800000090300020000000000
snmp-server group tapGroup v3 noauth read tapView write tapView
snmp-server view tapView ciscoIpTapMIB included
snmp-server view tapView cisco802TapMIB included
snmp-server view tapView ciscoTap2MIB included
snmp-server enable traps tty
snmp-server enable traps alarms informational
snmp-server manager


Router# show snmp user
User name: tapuser
```

```
Engine ID: 800000090300020000000000
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: tapGroup
```

Additional References

The following sections provide references related to the SII feature.

Related Documents

Related Topic	Document Title
SNMP configuration information	*Cisco IOS Configuration Fundamentals Configuration Guide,* Part 3: Cisco IOS System Management, "Configuring SNMP Support" section at: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html
SNMP command information	*Cisco IOS Network Management Command Reference , Release 12.2SB* at: http://www.cisco.com/en/US/docs/ios/netmgmt/command/ reference/nm_book.html
Lawful Intercept Architecture	*Lawful Intercept Architecture* http://www.cisco.com/en/US/docs/ios/sec_user_services/ configuration/guide/sec_lawful_intercept.html
PacketCable	PacketCable and PacketCable Multimedia for the Cisco CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm.html

MIBs

MIB	MIBs Link
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Service Independent Intercept

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 188: Feature Information for Service Independent Intercept

Feature Name	Releases	Feature Information
Service Independent Intercept	12.2(33)SCA	SII support is introduced and enhanced using SNMPv3 in Cisco IOS Release 12.2(33)SCA on the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 (with PRE2) universal broadband routers.
SII Routed CPE Support	12.2(33)SCF	SII Routed CPE Support feature was introduced.

Feature Name	Releases	Feature Information
IPv6 Address Packet Intercept	12.2(33)SCG	The IPv6 Address Packet Intercept feature supports lawful intercept of CMs and CPEs provisioned with IPv6 addresses. The following sections provide information about this feature: • IPv6 Address Packet Intercept, on page 1700 • Provisioning IPv6 Taps Using SNMPv3, on page 1712

CHAPTER 65

Subscriber Management Packet Filtering Extension for DOCSIS 2.0

First Published: December 17, 2008

Last Updated: November 16, 2009

The Cisco universal broadband router supports management of data packet filtering based on the subscriber's preferences and criteria. Packet filtering enhances security to the cable network by allowing only the specific packets to flow to the Customer Premise Equipment (CPE) while dropping the unwanted data packets from the cable network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring Subscriber Management Packet Filtering

The table shows the hardware compatibility prerequisites for the subscriber management packet filtering feature.

Table 189: Cable Hardware Compatibility Matrix for Subscriber Management Packet Filtering

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20 Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later Cisco uBR-MC3GX60V [141]

141 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

The software prerequisites for the subscriber management packet filtering feature are:

- The latest software image is loaded and working on the Cable Modem Termination System (CMTS) and the cable modems (CM).
- The configuration information on the main performance routing engine (PRE) and the standby PRE should be the same before the switchover.

Restriction for Configuring Subscriber Management Packet Filtering

- This feature can define up to 254 filtering groups. The number of filters in each group is 255.

Information About Configuring Subscriber Management Packet Filtering

A filter group specifies what filters are applied to the packets going to or coming from each specific CM or CPE device. It defines the rules or criteria to filter or drop a packet. Every packet that has to be filtered can either be accepted to send or filtered to be dropped. The criteria to filter a packet depends on the subscriber's preferences. The filter group can be applied to different subscriber management groups.

Cable subscriber management can be established using the following configuration methods:

- CMTS router configuration (via CLI)
- SNMP configuration

The process of configuring the subscriber management packet filtering is:

1. The packet filter group defines the action for a packet. The packet can be let to go to the CPE or dropped off the cable network based on the subscriber's packet criteria.
2. The CM sends a registration request to the CMTS. The registration request contains provisioning information that defines the association of a Packet Filtering Group (PFG) with the CM and its subscribers.
3. The specific downstream or upstream PFGs are used to bind the CM, CPE, embedded Multimedia Terminal Adaptor (eMTA), embedded Set-Top Box (eSTB) and embedded portal server (ePS) to a specific PFG.
4. The CMTS identifies the CPE device based on the CPE's DHCP information.

Note For the filter group to work for CMs, a CM must re-register after the CMTS router is configured.

How to Configure Subscriber Management Packet Filtering

This section describes the configuration tasks that are performed to manage subscriber packet filtering on the Cisco CMTS platforms. You can use the command-line interface (CLI) commands to complete the configuration.

Configuring the Filter Group

This section describes the tasks to configure the packet filter group. Follow the summary steps to complete the configuration.

To create, configure, and activate a DOCSIS filter group that filters packets on the basis of the TCP/IP and UDP/IP headers, use the cable filter group command in global configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 3	**cable filter group group-id index index-num [option option-value]** **Example:** `Router(config)# cable filter group 10 index 10 src-ip 10.7.7.7`	Creates, configures, and activates a DOCSIS filter group that filters packets.

Defining the Upstream and Downstream MTA Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for an embedded Multimedia Terminal Adaptor (eMTA.) Follow the summary steps to complete the configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	cable submgmt default filter-group mta {downstream | upstream} group-id **Example:** `Router(config)# cable submgmt default filter-group mta downstream 130`	Defines the upstream and downstream subscriber management filter groups for an MTA.

Defining the Upstream and Downstream STB Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for a Set-Top Box (STB.) Follow the summary steps to complete the configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	cable submgmt default filter-group stb {downstream | upstream} group-id **Example:** `Router(config)# cable submgmt default filter-group stb downstream 20`	Defines the upstream and downstream subscriber management filter groups for an STB.

Defining the Upstream and Downstream PS Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for a Portal Server (PS.) Follow the summary steps to complete the configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	cable submgmt default filter-group ps {downstream | upstream} group-id **Example:** `Router(config)# cable submgmt default filter-group ps downstream 10`	Defines the upstream and downstream subscriber management filter groups for a portal server.

Configuration Examples for Subscriber Management Packet Filtering

This section describes a sample configuration example for configuring the subscriber management packet filtering.

Configuring the Filter Group: Example

The following example shows configuration of a filter group that drops packets with a source IP address of 10.7.7.7 and a destination IP address of 10.8.8.8, and a source port number of 2000 and a destination port number of 3000. All protocol types and ToS and TCP flag values are matched:

```
Router(config)# cable filter group 10 index 10 src-ip 10.7.7.7
Router(config)# cable filter group 10 index 10 src-mask 255.255.0.0
Router(config)# cable filter group 10 index 10 dest-ip 10.8.8.8
Router(config)# cable filter group 10 index 10 dest-mask 255.255.0.0
Router(config)# cable filter group 10 index 10 ip-proto 256
Router(config)# cable filter group 10 index 10 src-port 2000
Router(config)# cable filter group 10 index 10 dest-port 3000
Router(config)# cable filter group 10 index 10 tcp-flags 0 0
Router(config)# cable filter group 10 index 10 match-action drop
```

Defining the Upstream and Downstream MTA Filter Group: Example

The following example shows configuration of an upstream and downstream MTA filter group.

```
Router# configure terminal
Router(config)# cable submgmt default filter-group mta downstream 10
```

Defining the Upstream and Downstream STB Filter Group: Example

The following example shows configuration of an upstream and downstream STB filter group.

```
Router#configure terminal
Router(config)#cable submgmt default filter-group stb downstream 20
```

Defining the Upstream and Downstream PS Filter Group: Example

The following example shows configuration of an upstream and downstream portal server filter group.

```
Router#configure terminal
Router(config)#cable submgmt default filter-group ps downstream 10
```

Additional References

The following sections provide references related to configuring the subscriber management packet filtering feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_release_notes_list.html

Standards

Standard	Title
None	

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

For information about commands, see the Cisco IOS CMTS Command Reference at http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html . For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the Cisco IOS Master Command List, All Releases, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html .

Feature Information for Subscriber Management Packet Filtering

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

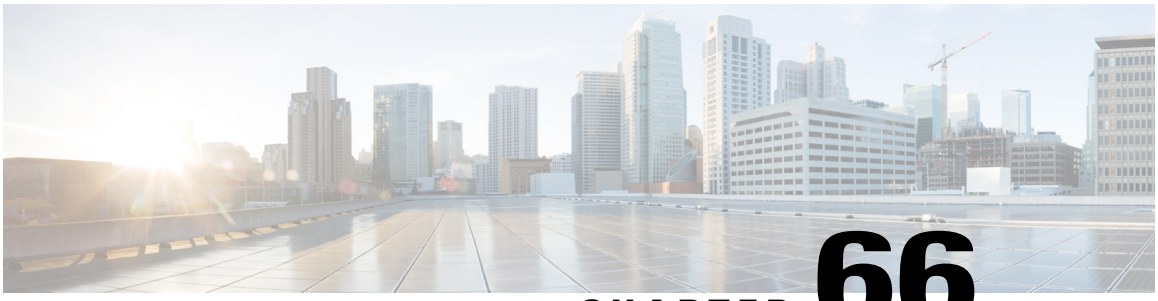
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 190: Feature Information for Subscriber Management Packet Filtering

Feature Name	Releases	Feature Information
Subscriber Management Packet Filtering	12.2(33)SCB	The Cisco universal broadband router supports management of data packet filtering based on the subscriber's preferences and criteria.

PART X

Troubleshooting and Network Management Features



CHAPTER 66

Automatic ROMMON Upgrade For Cable Interface Line Cards

First Published: June 20, 2011

Automatic ROM Monitor (ROMMON) Upgrade feature enables the Cisco uBR10012 cable interface line cards to automatically update the ROMMON image whenever a newer version is available. This document provides information about the Automatic ROMMON Upgrade feature and configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Automatic ROMMON Upgrade

Table 191: Cable Hardware Compatibility Matrix for Automatic ROMMON Upgrade for Cable Interface Line Cards, on page 1736 shows the hardware compatibility prerequisites for the Automatic ROMMON Upgrade feature.

Table 191: Cable Hardware Compatibility Matrix for Automatic ROMMON Upgrade for Cable Interface Line Cards

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2 • PRE4	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[142]

142 Cisco uBR-MC3GX60V cable interface line card is compatible with Performance Routing Engine 4 (PRE4).

Information About Automatic ROMMON Upgrade

The Cisco IOS Release 12.2(33)SCF introduces the Automatic ROMMON Upgrade feature, which enables the cable interface line cards (CLCs) to automatically upgrade the ROMMON image whenever a newer version is available.

The ROMMON is a bootstrap program that initializes the hardware and boots up the Cisco IOS software when the Cisco CMTS (or CLC) is powered on or rebooted. It is an integral part of the CLC firmware, which provides basic services such as CPU initialization, memory mapping, and image relocation.

Two types of ROMMON images exist on CLCs:

- Primary ROMMON image—This is the original image shipped with the system. This is a read-only image that cannot be erased or altered in the field. In case the secondary ROMMON image gets corrupted during upgrade, the primary ROMMON image is used to boot up the CLC.
- Secondary ROMMON image—This is a field upgradeable image which has the latest software version. This image is upgraded by the Automatic ROMMON Upgrade feature.

The ROMMON image may require updates due to feature additions or enhancements. The Automatic ROMMON Upgrade feature enables the CLC to upgrade the secondary ROMMON image without user intervention. The user is informed about the upgrade status through error or warning messages. For more information on the upgrade status, see Verifying Automatic ROMMON Upgrade on a Cable Interface Line Card, on page 1739.

Automatic upgrade of the secondary ROMMON image is performed only when the new image version is higher than the current secondary ROMMON image version. For example, if the secondary ROMMON image version is 160, then the ROMMON image upgrade will be performed only if the new image version is 161 or above.

New ROMMON versions are backward compatible. The updated ROMMON image can be used with the older Cisco IOS Release versions. If, for any reasons, older ROMMON version needs to be used, it is possible to downgrade the ROMMON image using the Automatic ROMMON Upgrade feature with few configuration changes.

To downgrade the ROMMON image, the following conditions must be met:

- The Cisco IOS Release version must support Automatic ROMMON Upgrade feature.
- Automatic ROMMON image downgrade must be enabled. See Enabling Automatic ROMMON Downgrade on Cable Interface Line Cards, on page 1738.
- The current ROMMON version should be higher than the downgrade version.

Note The updated ROMMON image may contain critical bug fixes and feature enhancements. It is recommended that the ROMMON image is not downgraded, unless it is necessary.

By default, the automatic ROMMON image upgrade and downgrade are disabled for all CLCs. Use the cable linecard auto-rommon-upgrade command to configure automatic ROMMON image upgrade on CLCs. Use cable linecard auto-rommon-downgrade command to configure automatic ROMMON image downgrade on CLCs.

Note Effective with Cisco IOS Release 12.2(33)SCF1, the automatic ROMMON image upgrade is enabled by default.

How to Configure Automatic ROMMON Upgrade on Cable Interface Line Cards

This section describes the following configuration procedures:

Enabling Automatic ROMMON Upgrade on Cable Interface Line Cards

This procedure describes how to enable or disable automatic upgrade of ROMMON images on CLCs.

Note The automatic ROMMON upgrade is disabled by default on all CLCs. To perform automatic ROMMON upgrade on the cable interface line cards, use the cable linecard auto-rommon-upgrade command to enable automatic ROMMON image upgrade on all the line cards and then reload the line cards.

Note Effective with Cisco IOS Release 12.2(33)SCF1, the automatic ROMMON image upgrade is enabled by default.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	cable linecard auto-rommon-upgrade **Example:** `Router(config)# cable linecard auto-rommon-upgrade`	Enables automatic ROMMON image upgrade on all CLCs. **Note** Use the no form of this command to disable automatic ROMMON image upgrade on CLC.
Step 4	end **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Examples to Enable Automatic ROMMON Image Upgrade

The following example shows how to enable automatic ROMMON image upgrade on all CLCs:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable linecard auto-rommon-upgrade
Router(config)# end
```

Enabling Automatic ROMMON Downgrade on Cable Interface Line Cards

This procedure describes how to enable or disable automatic downgrade of ROMMON images on CLCs.

Note The automatic ROMMON downgrade is disabled by default on all CLCs, and we recommend that you do not change this default behavior.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	cable linecard auto-rommon-downgrade **Example:** `Router(config)# cable linecard auto-rommon-downgrade`	Enables automatic ROMMON image downgrade on all CLCs. **Note** Use the no form of this command to disable automatic ROMMON image downgrade on CLC.
Step 4	end **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Examples for Automatic ROMMON Image Downgrade

The following example shows how to enable automatic ROMMON image downgrade on all CLCs:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable linecard auto-rommon-downgrade
Router(config)# end
```

Verifying Automatic ROMMON Upgrade on a Cable Interface Line Card

On successful automatic ROMMON upgrade (or downgrade), the following two messages are observed in system logs:

- %UBR10KCLC-6-ROMMON_UPDATE_START
- %UBR10KCLC-6-ROMMON_UPDATE_DONE

For more information on these system messages, see the Cisco IOS CMTS Cable System Messages Guide at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

Troubleshooting Automatic ROMMON Upgrade failures

If automatic ROMMON image upgrade (or downgrade) fails, system error messages indicating one of the following reasons are observed in the system logs:

- ROMMON update disabled—Line card ROMMON update is temporarily disabled due to a limit on unsuccessful attempts. The card may not have the latest firmware
- ROMMON version error—Line card ROMMON version error. The line card may not have the latest version.
- ROMMON update error—Line card ROMMON update error. The line card ROMMON update can fail due to any one of the following reasons:
  - Failure to erase old firmware on the line card.
  - Failure to program new firmware.
  - Line card not responding.
  - Line card timeout.
  - Memory related failure.

If any of these syslog error messages are observed, wait for 10 minutes and then try to reload the CLC. For more information on how to reload a CLC, see:

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

If the problem persists collect the output of the show tech-support command. Contact your Cisco technical support representative and provide the representative with the gathered information.

For more information on the exact system error messages observed during ROMMON upgrade (or downgrade) failure, see the Cisco IOS CMTS Cable System Messages Guide at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco CMTS System Messages Guide	Cisco IOS CMTS Cable System Messages Guide http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

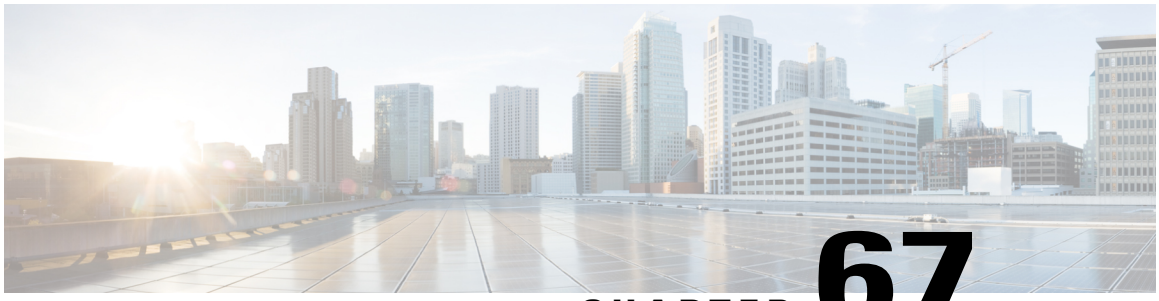
Feature Information for Automatic ROMMON Upgrade

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 192: Feature Information for Automatic ROMMON Upgrade for Cable Interface Line Card

Feature Name	Releases	Feature Information
Automatic ROMMON Upgrade for Cable Interface Line Cards	12.2(33)SCF	This feature enables the Cisco uBR10012 cable interface line cards to automatically perform ROMMON image upgrade or downgrade. The following commands were introduced: • **cable linecard auto-rommon-upgrade** • **cable linecard auto-rommon-downgrade**



CHAPTER 67

Cable IPC Statistics Collection Tool

First Published: November 16, 2009

Last Updated: November 29, 2010

The Cable Interprocess Communication (IPC) Statistics Collection tool provides debugging information about all CMTS related IPC messages. You can use this tool to analyze the IPC traffic in a cable communications network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Cable IPC Statistics Collection Tool

The table shows the hardware compatibility prerequisites for the Cable IPC Statistics Collection tool.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 193: Hardware Compatibility Matrix for Cable IPC Statistics Collection Tool

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [143]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [144]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

143 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

144 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for the Cable IPC Statistics Collection Tool

The Cable IPC Statistics Collection tool has the following restrictions:

- Does not support the line cards running LCDOS images.
- Does not support checkpoint messages between the primary route processor (RP) and secondary RP on the Cisco UBR10012 router.

Information About the Cable IPC Statistics Collection Tool

The Cable IPC Statistics Collection tool monitors IPC messages between cable interface line cards and the RP in a cable communications network. The IPC messages include configuration commands, responses to the configuration commands, and other events that a cable interface line card reports to the RP.

The tool provides the following message statistics:

- Send and receive message counts and byte counts.
- Wait time between request sent and response received for blocked request messages.
- Process time used by the message handler for received request messages.

The tool provides the following queue statistics:

- Queue size.
- Wait time from a message that is enqueued to a message that is dequeued.
- Enqueue and dequeue message counts.
- Queue flush message counts.

Note To save system memory and keep the normal operation performance, the Cable IPC Statistics Collection tool is disabled by default. You can enable the tool using the cable ipc-stats command in global configuration mode. When you enable the tool, a new database memory buffer is allocated, and the API functions start updating the statistics database. When you disable the tool, the allocated memory is freed. We recommend that you enable this tool only when it is necessary as the tool consumes considerable amount of CPU memory while running on a Cisco CMTS router. The actual memory usage varies based on how many messages are defined in a particular Cisco IOS image.

How to Enable the Cable IPC Statistics Collection Tool

This section contains the following procedures:

Enabling the Cable IPC Statistics Collection Tool

The cable ipc-stats command is synchronized to all cable interface line cards from the active RP. You do not have to use this command on cable interface line cards separately.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable ipc-stats** **Example:** `Router(config)# cable ipc-stats`	Enables the Cable IPC Statistics Collection tool on a Cisco CMTS router.

Verifying IPC Statistics

To verify IPC statistics, use the **show cable ipc-stats** command as shown in the following example:

```
Router# show cable ipc-stats
ubr10k2apatil#show cable ipc-stats
--- TIME ---
Start: 03:27:29 PDT Fri Oct 9 2009
End  : 03:28:22 PDT Fri Oct 9 2009
Total: 0 days 00 hrs 00 mins 53 secs (53 seconds)
size : 1407648 bytes
--- CR10K MSG ---
entity app      io    s/s reqid idx:    pkts      bytes lastEvt totalDur maxDur lastMax
                                                        (sec)   (msec)   (msec) (sec)
rp-lc c10k     TxReq 1/0 10241   1:       1         24      17
 rp-lc c10k     TxReq 1/0    10  14:      11        704       0
 rp-lc c10k     TxReq 2/1    10  14:      10        640       4
 rp-lc c10k     TxReq 3/0    10  14:      10        640       4
 rp-lc c10k     TxReq 3/1    10  14:      11        704       0
 rp-lc c10k     TxReq 4/0    10  14:      10        640       3
 rp-lc c10k     TxReq 6/0 10252   2:      10       9376      13
 rp-lc c10k     TxReq 6/0    10  14:      11        704       0
 rp-lc c10k     TxReq 6/1 10252   2:       1         88      53
 rp-lc c10k     TxReq 6/1    10  14:      11        704       0
 rp-lc c10k     TxReq 7/0 10252   2:       7        696       5
 rp-lc c10k     TxReq 7/0    10  14:      11        704       1
 rp-lc c10k     RxRsp 1/0 10241   1:       1          4      17        0       0 17
 rp-lc c10k     RxReq 1/0 10241   1:      60      21816       0        0       0 0
 rp-lc c10k     RxReq 1/0    10  14:      11        704       0        0       0 0
 rp-lc c10k     RxReq 2/1 10241   1:      26      13468       1        0       0 1
 rp-lc c10k     RxReq 2/1    10  14:      10        640       4        0       0 4
 rp-lc c10k     RxReq 3/0 10241   1:      20       1340       5        0       0 5
 rp-lc c10k     RxReq 3/0    10  14:      10        640       4        0       0 4
 rp-lc c10k     RxReq 3/1    10  14:      11        704       0        0       0 0
 rp-lc c10k     RxReq 4/0 10241   1:      20       1340       9        0       0 9
 rp-lc c10k     RxReq 4/0    10  14:      10        640       3        0       0 3
 rp-lc c10k     RxReq 6/0 10252   2:      13      27080       0        0       0 0
 rp-lc c10k     RxReq 6/0    10  14:      11        748       0        0       0 0
```

```
 rp-lc c10k     RxReq 6/1 10252   2:       1         68       25         0       0 25
 rp-lc c10k     RxReq 6/1    10  14:      11        748        0         0       0 0
 rp-lc c10k     RxReq 7/0 10252   2:      11      24548        3         0       0 3
 rp-lc c10k     RxReq 7/0    10  14:      11        748        1         0       0 1
 rp-lc pnego    TxReq 6/0    14   6:       3        363       13
 rp-lc pnego    TxReq 6/1    14   6:       1         30       53
 rp-lc pnego    TxReq 7/0    14   6:       2         62       13
 rp-lc plfm     RxReq 6/0    24  17:       1         12       37         0       0 37
 rp-lc plfm     RxReq 6/0    27  20:      11       1144        0         0       0 0
 rp-lc plfm     RxReq 6/0    28  21:     484      19360        0         0       0 0
 rp-lc plfm     RxReq 6/1    24  17:       1         12       25         0       0 25
 rp-lc plfm     RxReq 7/0    24  17:       1         12       45         0       0 45
 rp-lc plfm     RxReq 7/0    27  20:      10       1040        3         0       0 3
 rp-lc plfm     RxReq 7/0    28  21:     440      17600        3         0       0 3
 rp-lc docsis   TxReq 7/0   118 110:      10         80        5
 rp-lc hccp     TxReq 6/0     8   8:       8       8416       13
 rp-lc hccp     RxReq 6/0     2   2:       1         28       13         0       0 13
--- CR10K TXQ ---
 TXQ_6_0
 enQ: 10 pkts  max Q size 9 at 13 sec ago
 deQ: 10 pkts  max delay 24 msec at 13 sec ago
   delay between (  0,  10) msec:        6 pkts
   delay between ( 10,  20) msec:        3 pkts
   delay between ( 20,  30) msec:        1 pkts
   delay between (  0,   1) sec :       10 pkts
 flush: 0 ptks  0 times
 TXQ_6_1
 enQ: 1 pkts  max Q size 1 at 53 sec ago
 deQ: 1 pkts  max delay 0 msec at 53 sec ago
   delay between (  0,  10) msec:        1 pkts
   delay between (  0,   1) sec :        1 pkts
 flush: 0 ptks  0 times
 TXQ_7_0
 enQ: 7 pkts  max Q size 1 at 5 sec ago
 deQ: 7 pkts  max delay 48 msec at 13 sec ago
   delay between (  0,  10) msec:        1 pkts
   delay between ( 10,  20) msec:        5 pkts
   delay between ( 40,  50) msec:        1 pkts
   delay between (  0,   1) sec :        7 pkts
 flush: 0 ptks  0 times
--- CR10K WATERMARK ---
--- CR10K RXQ ---
 c10k rxq
 enQ: 236 pkts  max Q size 3 at 5 sec ago
 deQ: 236 pkts  max delay 4 msec at 35 sec ago
   delay between (  0,  10) msec:      236 pkts
   delay between (  0,   1) sec :      236 pkts
 flush: 0 ptks  0 times
 cr10k LP rxq
 enQ: 25 pkts  max Q size 1 at 0 sec ago
 deQ: 25 pkts  max delay 0 msec at 0 sec ago
   delay between (  0,  10) msec:       25 pkts
   delay between (  0,   1) sec :       25 pkts
 flush: 0 ptks  0 times
```

Note When you run the show cable ipc-stats command, a separate shadow database buffer is allocated, and the contents of the active database are copied to the shadow database to display the IPC statistics. This ensures that all the statistics are frozen at the same time for easy comparison and analysis. To clear the active database, use the clear cable ipc-stats command in privileged EXEC mode. This command resets all the statistics in the active database to zero.

Configuration Example for the Cable IPC Statistics Collection Tool

The following example shows how to configure the Cable IPC Statistics Collection Tool on a Cisco CMTS router:

```
Router# configure terminal
Router(config)# cable ipc-stats
```

Additional References

The following sections provide references related to the Cable IPC Statistics Collection tool feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband) routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
IPC messages	*Cisco IOS CMTS Cable System Messages Guide* http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

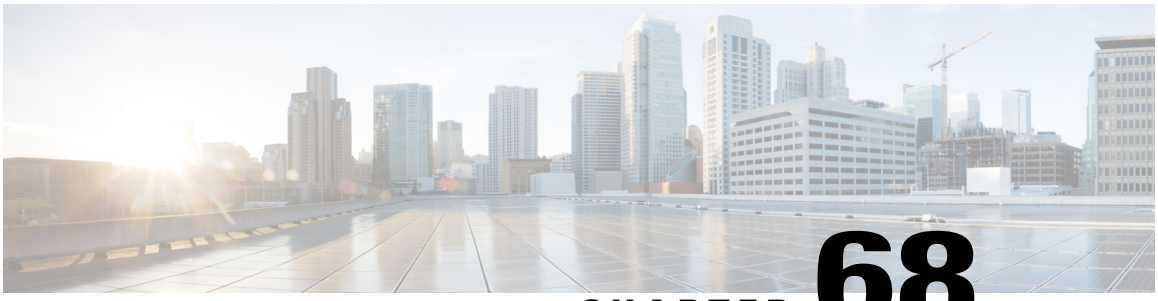
Feature Information for the Cable IPC Statistics Collection Tool

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 194: Feature Information for the Cable IPC Statistics Collection Tool

Feature Name	Releases	Feature Information
Cable IPC Statistics Collection tool	12.2(33)SCC	The Cable IPC Statistics Collection tool provides debugging information about all IPC messages. The following sections provide information about this feature: The following commands were introduced: • **cable ipc-stats** • **clear cable ipc-stats** • **show cable ipc-stats**



CHAPTER 68

Cisco CMTS Static CPE Override

First Published: February 14, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the commands and guidelines for using the Cisco CMTS Static CPE Override feature. This feature enables service technicians to override Dynamic Host Configuration Protocol (DHCP) settings on a subscriber's Customer Premise Equipment (CPE) devices. This feature is used for troubleshooting purposes and to assign static IP addresses at a customer's facility while retaining full and uninterrupted support from the Cisco CMTS.

The cable submgmt default command enables Multiple Service Operators (MSOs) to override network DHCP settings in the Cisco Cable Modem Termination System (CMTS) when performing troubleshooting with a laptop computer from end user facilities.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for CMTS Static CPE Override

- Cisco IOS software release 12.3(9a)BC or a later BC train release
- A laptop computer
- Ethernet connection cabling
- Remote console access to the Cisco CMTS

Restrictions for CMTS Static CPE Override

Cisco CMTS Static CPE Override is disabled by default, and is enabled with the cable submgmt default command. This feature has the following intentional restrictions:

- This feature supports additional CPE devices with additional MAC addresses to share the IP address and service ID (SID) with the original CPE device. However, CPE devices are limited to 1024 and beyond that, are not supported nor allowed.
- The original CPE device (with the original MAC address and SID) is not allowed behind a different cable modem with the original IP address. If this restriction were not in place, the original cable modem (with the original IP address and SID) would experience interrupted service.
- The original CPE device (with the original MAC and IP address) is not allowed to support a second SID or IP address through a second cable modem.

The impact of this restriction is as follows:

- ◦ A field technician's laptop is allowed to assume an existing IP address and service ID (SID) behind a cable modem on-site.
- At the end of an on-site service session, the CPE device must reclaim its IP address again via DHCP. If this does not occur, the Cisco CMTS presumes that the technician's laptop remains behind the previous cable modem, and the Static CPE override feature will not be available for a future on-site session at another location.

You can override this state with either of the following two methods:

- ◦ Clear the technician's CPE device information from the host routing tables on the Cisco CMTS.
  ◦ Ensure that at the end of an on-site troubleshooting session, the original CPE device reclaims its IP address using DHCP. The technician's (temporary) CPE entry is automatically deleted.

Information About CMTS Static CPE Override

One typical scenario in which DHCP is used with the Cisco CMTS and CPE devices would include the following:

- A CPE device is configured with a dynamic IP address via DHCP from the Cisco CMTS.
- A CPE MAC address is configured behind the cable modem with a service ID (SID) assigned to the IP address.

In this scenario, the cable submgmt default command can be used on the Cisco CMTS to accomplish the following (temporary) changes between the CPE devices and the Cisco CMTS:

- The original CPE device continues to receive service, but is assigned a static IP address from the Cisco CMTS.
- This static IP address overrides the DHCP IP address without first clearing the DHCP CPE device from the CMTS routing tables.
- 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.
- Additional CPE devices can now share the same IP address and SID as the original CPE device.

How to Configure Cisco CMTS Static CPE Override

This section contains the following procedures for the Cisco CMTS Static CPE Override feature:

Enabling and Using Cisco CMTS Static CPE Override

Perform the following steps to enable Cisco CMTS Static CPE Override, and to enable network access of a second CPE device behind a subscriber's cable modem at the customer facility.

Before You Begin

This procedure requires that the field technician already have connected and started a laptop computer at the customer facilities, is connected through the customer's cable modem, and has accessed the Cisco CMTS with remote router console.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# config t`	Enters global configuration mode.
Step 3	cable submgmt default active **Example:** `Router(config)# cable submgmt default active`	Enables the Cisco CMTS Static CPE Override feature behind the subscriber's cable modem. Additional CPE devices (with additional MAC addresses) are supported behind the subscriber's cable modem, and they inherit the subscriber's current SID settings. **Note** The subscriber's CPE device changes from dhcp cpe to static CPE in the CMTS host table.
Step 4	cable submgmt default filter-group cm (downstream | upstream) **Example:** `Router(config)# cable submgmt default filter group cm downstream`	Enables one or more temporary CPE devices behind a subscriber's cable modem to operate within the cable modem's downstream or upstream filter group.
Step 5	cable submgmt default filter-group cpe {downstream | upstream} **Example:** `Router(config)# cable submgmt default filter-group cpe upstream`	Enables one or more temporary CPE devices behind a subscriber's cable modem to operate within the subscriber's CPE downstream or upstream filter group.
Step 6	cable submgmt default learnable **Example:** `Router(config)# cable submgmt default learnable`	Enables one or more temporary CPE devices behind a subscriber's cable modem to learn and operate within the routing table defined on the Cisco CMTS.
Step 7	cable submgmt default max-cpe n **Example:** `Router(config)# cable submgmt default max-cpe 1024`	Sets the maximum number of CPE devices to be allowed behind a subscriber's cable modem. • n—The number of allowable CPE devices in addition to the subscriber's CPE device(s), with a range from 0 to 1024 devices. Each device inherits the SID settings as defined by the subscriber's current SID.
Step 8	interface slot/[subslot]/port **Example:** `Router(config)# interface 8/1/0`	Enters interface configuration mode for the specified interface. The subslot is required syntax for the Cisco uBR10012 router, but is not used for the Cisco uBR7246VXR or Cisco uBR7100 series routers.

	Command or Action	Purpose
Step 9	(no) ip address ip-address mask [secondary] **Example:** `Router(config-if)# ip address 131.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for a CPE device, use the ip address command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command. ip address ip-address mask [secondary] no ip address ip-address mask [secondary] • ip-address—Static IP address for the CPE device. • mask—Mask for the associated IP subnet. • secondary—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
Step 10	Conduct on-site CPE troubleshooting, as required.	For additional troubleshooting guidelines, refer to the Troubleshooting Tips, on page 1789.
Step 11	Ctrl-Z **Example:** `Router(config-if)# Ctrl^z`	As required, return to global configuration mode.
Step 12	Do one of the following: • no cable submgmt default • • clear cable host **Example:** `Router(config)# cable submgmt default` **Example:** `Router(config)# clear cable host`	Disables Static CPE override, and returns the on-site CPE device(s) and cable modem to their original DHCP state (dynamic IP address with associated SID). To clear the CPE cable modem host from the Cisco router's internal address tables, use the clear cable host command in privileged EXEC mode. clear cable host {ip-address | mac-address} • ip-address—IP address for the device to be cleared. • mac-address—MAC address for the device to be cleared. For additional command information, refer to the clear cable command in the Cisco Broadband Cable Command Reference Guide on Cisco.com.
Step 13	exit **Example:** `Router(config)# exit`	Returns the prompt to privileged EXEC mode.
Step 14	**quit**	Proper Telnet reconnection to the Cisco router requires proper disconnect during the current Telnet session. Common Telnet disconnect methods are as follows: • Press Ctrl+Break. • Press Ctrl+].

	Command or Action	Purpose
		• Type quit or send break. Another Telnet disconnect method is as follows: Press Ctrl+Shift 6 6 x. For additional Telnet break sequences, refer to the document Standard Break Key Sequence Combinations During Password Recovery on Cisco.com.
Step 15	Type disc 1 from the router command-line interface.	

Examples

The command in 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 command in 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 command in 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 command in 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
```

Troubleshooting with Cisco CMTS Static CPE Override

When Cisco CMTS Static CPE Override has been enabled at the subscriber's facilities, troubleshooting depends on the service or network needs of the situation. For additional information about troubleshooting the Cisco CMTS or customer CPE devices, refer to the Additional References, on page 1756.

Additional References

The following sections provide references related to CPE troubleshooting with the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
CPE troubleshooting information	• *Cisco TAC Technical Notes for the Cisco CMTS:* http://www.cisco.com/c/en/us/tech/broadband-cable/cable-modem-termination-systems-cmts/tech-tech-notes-list.html • *Removing Cable Modem and CPE Entries from the Cisco CMTS, TAC Document ID 4663* http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/4663-cm-cpe-entries-removed.html • *Troubleshooting Slow Performance in Cable Modem Networks, TAC Document ID 12551:* http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/12551-troubleshooting-slow-perf.html • Troubleshooting uBR Cable Modems Not Coming Online, TAC Document ID 16510 http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/16510-troubleshooting-cm-online.html
DHCP configuration information	• "DHCP, ToD, and TFTP Services for the Cisco CMTS" in the Cisco Cable Modem Termination System Feature Guide: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_dhcp.htm

Standards

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

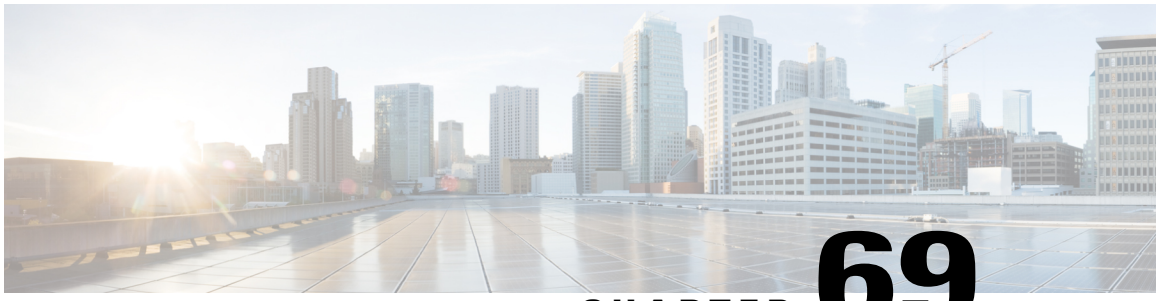
Feature Information for CMTS Static CPE Override

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 195: Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Cisco CMTS Static CPE Override	12.2(33)S	The following command is introduced or modified in the feature or features documented in this module. • **cable submgmt default**



CHAPTER 69

Control Point Discovery on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: December 17, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Control Point Discovery (CPD) feature. This feature, along with Network Layer Signaling (NLS), enables automatic discovery of any control point associated with an end point.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Control Point Discovery

The Control Point Discovery feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table shows the hardware compatibility prerequisites for this feature.

Table 196: Control Point Discovery Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE-2	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Restrictions for Control Point Discovery

- The CPD feature does not sync any dynamic CPD/NLS related data between the route processors (RPs). After sending a NLS challenge to the controller, the new active PRE will ignore the NLS response as a result of any RP switchover.
- The CPEs become inaccessible for a small duration during line card switchovers. During this interval, any CPD request received on CMTS will be responded to as if the endpoint is not connected or as if the control relationship is not supported.
- The CPD functionality is restricted to default VPN table id (0).
- Only manual configuration of NLS authentication pass phrase would be supported for CPD/NLS security.
- For NLS authentication, HMAC SHA1 (no configuration option) is used with MAC length truncated to 96 bits.

Information About Control Point Discovery

To configure the Control Point Discovery feature, you should understand the following concepts:

Control Points

Control points are points in a network that can be used to apply certain functions and controls for a media stream. In a cable environment, the control points are Cable Modem Termination Systems (CMTS) and devices that utilizes these control points are referred to as CPD Requestors (or controllers).

Cable CPD Requestors include the following:

- Call Management Server (CMS)
- Policy Server (PS)
- Mediation Device for Lawful Intercept (MD)

Network Layer Signaling (NLS)

Network Layer Signaling (NSL) is an on-path request protocol used to carry topology discovery and other requests in support of various applications. In the CPD feature, NLS is used to transport CPD messages.

NLS for CPD

NLS is used to transport CPD messages. The CPD data is carried under an application payload of the NLS and contains a NLS header with flow id. The NLS flow id is used during NLS authentication to uniquely identify the CPD requests and responses for an end point of interest.

NLS Flags

All NLS headers contain bitwise flags. The CMTS expects the following NLS flag settings for CPD applications:

- HOP-BY-HOP = 0
- BUILD-ROUTE = 0
- TEARDOWN = 0
- BIDIRECTOINAL = 0
- AX_CHALLANGE = 0/1
- AX_RESPONSE = 0/1

Note Any requests with flags other then AX flags, set to one will be rejected with an error indicating a poorly formed message.

NLS TLVs

The following NLS TLVs are supported for all CPD applications:

- APPLICATION_PAYLOAD
- IPV4_ERROR_CODE
- IPV6_ERROR_CODE
- AGID

- A_CHALLENGE
- A_RESPONSE
- B_CHALLENGE
- B_RESPONSE
- AUTHENTICATION
- ECHO

The following NLS TLVs are not supported for CPD applications:

- NAT_ADDRESS
- TIMEOUT
- IPV4_HOP
- IPV6_HOP

Control Point Discovery

The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint.

Using Networking Layer Signaling (NLS), the control point discovery feature sends a CPD message towards the end point (MTA). The edge/aggregation device (CMTS), located between the requestor and the endpoint, will respond to the message with its IP address.

Note For Lawful Intercept, it is important that the endpoint does not receive the CPD message. In this instance, the CMTS responds to the message without forwarding it to its destination.

CPD Protocol Hierarchy

CPD messages are sent over the NLS.

The CPD Protocol Hierarchy is as follows:

1. CPD
2. NLS
3. UDP
4. IP

Note Since NLS is implemented on the UDP protocol, there is a potential of message loss. If messages are lost, the controller will re-send the CPD request in any such event.

Control Relationship

A control relationship between a control point and a controller is identified as a function on a media flow that passes through a control point. A control relationship is uniquely defined by a control relationship type (CR TYPE) and control relationship ID (CR ID). The CR ID is provisioned on CMTS as well as the controller.

The table lists the supported CR TYPEs and corresponding pre-defined CR IDs

Table 197: Supported Control Relationship Types and Corresponding Control Relationship IDs

Control Relationship Type	Pre-Defined Corresponding Control Relationship ID
CR TYPE = 1 (Lawful Intercept)	CR ID = 1: CMTS
	CR ID = 2: Aggregation router or switch in front of CMTS
	CR ID = 3: Aggregation router or switch in front of Media Services
	CR ID = 4: Media Gateway
	CR ID = 5: Conference Server
	CR ID = 6: Other
CR TYPE = 2 (DQoS)	CR ID = 1: CMTS
CR TYPE = 3 (PCMM)	CR ID = 1: CMTS

How to Configure CPD

Enabling CPD Functionality

To enable the CPD functionality, use the cpd command in global configuration mode. The CPD message authentication is determined by NLS configuration.

Before You Begin

The CPD message authentication is determined by NLS configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cpd** **Example:** `Router (config)# cpd`	Enables CPD functionality • Us the “no” form of this command to disable CPD functionality.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples for CPD Enable

The following example shows the cpd enabled on a router:

```
Router (config)# cpd
```

Configuring Control Relationship Identifier

To configure a Control relationship identifier (CR ID) for CMTS, use the cpd cr-id command. When CPD request comes with a wild-card CR ID, the CMTS will respond with this configured value.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cpd cr-id** **Example:** `Router (config)# cpd cr-id 100`	Configures a control relationship identifier (CR ID) for CMTS.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the cpd cr-id command configured with a cr-id number of 100 on a router.

```
Router (config)# cpd cr-id 100
```

Enabling NLS Functionality

To enable the NLS functionality, use the nls command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**nls** **Example:** `Router (config)# nls`	Enables NLS functionality. • NLS authentication is optional. • It is recommended that NLS message authentication be enabled at all times.
Step 4	**debug nls** **Example:** `Router# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls command enbaled on a router.

```
Router (config)# nls
```

Configuring Authorization Group Identifier and Authentication Key

The Authorization Group Identifier (AG ID) and corresponding authorization key are provisioned on CMTS, as well as on controller/CPD requester.

To configure the Authorization Group Identifier and Authentication Key, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls ag-id** **Example:** `Router (config)# nls ag-id 100 auth-key 20`	Configures the Authorization Group Identifier and Authentication Key.
Step 4	**debug nls** **Example:** `Router (config)# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls ag-id command with an Authorization Group ID of 100 and Authentication Key of 20.

```
Router (config)# nls ag-id 100 auth-key 20
```

Configuring NLS Response Timeout

The NLS response timeout governs the time CMTS will wait for getting a response for a NLS authentication request.

To configure the NLS response timeout, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls resp-timeout** **Example:** `Router (config)# nls resp-timeout 60`	Configures the NLS response time.
Step 4	**debug nls** **Example:** `Router (config)# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls resp-timeout command with a response timeout setting of 60 seconds.

```
Router (config)# nls resp-timeout 60
```

Additional References

The following sections provide references related to the CPD feature.

Related Documents

Related Topic	Document Title
CMTS features	• *Cisco IOS CMTS Cable Software Configuration Guide* • Managed Broadband Access Using MPLS VPNs for Cable Multiservice Operators • Transparent LAN Service over Cable • Troubleshooting the System

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Standards

Standard	Title
Internet Draft, Network Layer Signaling: Transport Layer	Internet Draft, Network Layer Signaling: Transport Layer (IETF draft-shore-nls-tl-05.txt)
PacketCable™ Control Point Discovery Interface Specification	PacketCable™ Control Point Discovery Interface Specification (PKT-SP-CPD-I02-061013)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Control Point Discovery

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 198: Feature Information for Control Point Discovery

Feature Name	Releases	Feature Information
Control Point Discovery	12.3(21a)BC3	The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint. The following commands were introduced or modified by this feature: • **cpd** • **cpd cr-id** • **debug cpd** • **debug nls** • **nls** • **nls ag-id auth-key** • **nls resp-timeout** • **show cpd** • **show nls** • **show nls ag-id** • **show nls flow**
Control Point Discovery	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.

CHAPTER 70

Flap List Troubleshooting for the Cisco CMTS

First Published: February 14, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure and use the Flap List Troubleshooting feature on the Cisco Cable Modem Termination System (CMTS) routers. The flap list is a patented tool for the Cisco CMTS routers to diagnose potential problems with a particular cable modem or with a particular cable interface. The flap list tracks “flapping” cable modems, which are cable modems that have intermittent connectivity problems. Excessive flapping could indicate a problem with a particular cable modem or with the upstream or downstream portion of the cable plant.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Flap List Troubleshooting

- To configure and access the flap list using SNMP commands, you must be using an SNMPv3 manager and have configured the Cisco CMTS router for SNMP operations.

Restrictions for Flap List Troubleshooting

- The Cisco CMTS should be running the latest Cisco IOS Release 12.1 EC or Cisco IOS Release 12.2 EC, or later, release.
- The Flap List Troubleshooting feature can be used only with two-way cable modems. The flap-list does not support telco-return cable modems or set-top boxes.

Note Since the cable flap list was originally developed, polling mechanisms have been enhanced to have an increased rate of 1/sec when polls are missed. Cable modems can go offline faster than the frequency hop period, which can cause the frequency to stay fixed while cable modems go offline. To compensate for this, reduce the hop period to 10 seconds.

Information About Flap List Troubleshooting

This section describes the following information about the Flap List Troubleshooting feature:

Feature Overview

The Flap List Troubleshooting is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) routers. The flap list tracks “flapping” cable modems, which are cable modems that have intermittent connectivity problems. A flapping cable modem can indicate either a problem with that particular cable modem, or it could indicate an RF noise problem with the upstream or downstream portion of the cable plant.

The flap-list feature supports any cable modem that conforms to the Data-over-Cable Service Interface Specifications (DOCSIS) because it does use any special messaging to poll cable modems or to request any special information from them. Instead, this feature monitors the normal registration and station maintenance activity that is already performed over a DOCSIS cable network.

This allows the Cisco CMTS to collect the flap-list data without generating additional packet overhead and without impacting network throughput and performance. It also means that although the Flap List Troubleshooting feature is a proprietary feature for Cisco CMTS routers, it is compatible with all DOCSIS-compliant cable modems. In addition, unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

Information in the Flap List

The Flap List Troubleshooting feature tracks the following situations:

- Reinsertions—A reinsertion occurs when the cable modem re-registers more frequently than the user-specified insertion time. A pattern of reinsertions can indicate either potential problems in the downstream or that the cable modem is being improperly provisioned.
- Hits and Misses—A hit occurs when a cable modem successfully responds to the station maintenance messages (MAC-layer "keepalive" messages) that the Cisco CMTS sends out to conform to the DOCSIS standard. A miss occurs when the cable modem does not respond to the request within the user-specified timeout period. A pattern of misses can indicate a potential problem in either the downstream or upstream path, or that a problem can be occurring in the registration process.
- Power Adjustments—DOCSIS cable modems can adjust their upstream transmission power levels to adjust to unstable cable plant signal levels, up to a maximum allowable power level. Repeated power adjustments usually indicate a problem with an amplifier in the upstream return path.

The flap-list feature is automatically enabled, but to use the flap list effectively, the cable system administrator should also typically do the following:

- Set up a script to periodically poll the flap list, for example, every 15 minutes.
- Examine the resulting data and perform trend analysis to identify cable modems that are consistently in the flap list.
- Query the billing and administrative database for cable modem MAC address-to-street address translation and generate a report. The reports can be given to the customer service department or the cable plant's operations and maintenance department. Using these reports, maintenance personnel can quickly discern how characteristic patterns of flapping cable modems, street addresses, and flap statistics indicate which amplifier or feeder lines are faulty. The reports also help to quickly discern whether problems exist in your downstream or upstream path and whether the problem is ingress noise or equipment related.

The flap list provides a quick way to quickly diagnose a number of possible problems. For example, if a subscriber reports a problem, but the flap list for the cable interface that is providing services to them shows little or no flap-list activity, the cable technician can assume that the Cisco CMTS and cable plant are communicating reliably. The problem, therefore, is probably in the subscriber's computer equipment or in the local connection to the cable modem.

Similarly, a cable technician can use the pattern of reinsertions, hits and misses, and power adjustments to quickly troubleshoot the following types of problems:

- If a subscriber's cable modem shows a lot of flap-list activity, it is having some kind of communication problem. Either the cable modem's hardware is faulty, its installation is faulty, the coaxial cable being used is faulty, or some portion of the cable plant that services this cable modem is faulty.
- Focus on the top 10 percent of cable modems that are most active in the flap list, since these are the most likely to indicate consistent and pervasive plant or equipment problems that will continue to disrupt communication with the headend.
- Cable modems with more than 50 power adjustments per day have a suspect upstream path.
- Cable modems with approximately the same number of hits and misses and with a lot of insertions have a suspect downstream path (for example, low level into the cable modem).

- All cable modems incrementing the insertion at the same time indicates a problem with the provisioning servers.
- Cable modems with high cyclic redundancy check (CRC) errors have bad upstream paths or in-home wiring problems.
- Correlating cable modems on the same physical upstream port with similar flap-list statistics can quickly resolve outside plant problems to a particular node or geography.

In addition, the cable network administrators can use the flap list to collect quality control and upstream performance data. Typically, the network operations center (NOC) saves the flap list to a database on a local computer on a daily basis, providing the ability to generate reports that track upstream performance and installation quality control, as well as to provide trend reports on cable plant problems.

Tip The system supports automatic power adjustments. The show cable flap-list and show cable modem commands indicate when the headend cable router has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (*) appears in the power-adjustment field for a modem when a power adjustment has been made; an exclamation point (!) appears when the modem has reached its maximum power-transmit level and cannot increase its power level any further.

Cisco Cable Manager and Cisco Broadband Troubleshooter

The Flap List Troubleshooting feature is supported by Cisco Cable Manager (CCM), Release 2.0 or later, which is a UNIX-based software suite that manages routers and DOCSIS-compliant cable modems, generates performance reports, troubleshoots connectivity problems, views the network graphically, and edits DOCSIS configuration files. You can access the CCM locally from the CCM server console or remotely from a UNIX workstation or a PC.

The Flap List Troubleshooting feature also works together with the Cisco Broadband Troubleshooter (CBT), which is a graphical-based application to manage and diagnose problems on the hybrid fiber-coaxial (HFC) network. Radio frequency (RF) technicians can quickly isolate plant and provisioning problems and characterize upstream and downstream trouble patterns, including analyzing flapping modems.

Benefits

The Flap List Troubleshooting feature is a proactive way to manage and troubleshoot problems on an HFC network. Its use of passive monitoring is more scalable and efficient than techniques that send special messages to cable modems or that regularly poll the cable modems using Simple Network Management Protocol (SNMP) commands. Because it uses mechanisms that already exist in a DOCSIS network, it can be used with any DOCSIS-certified cable modem or set-top box.

The flap list provides a cable technician with both real-time and historical cable health statistics for quick, accurate problem isolation and network diagnosis. Using the flap list, a cable technician is able to do the following:

- Quickly learn how to characterize trouble patterns in the hybrid fiber-coaxial (HFC) network.
- Determine which amplifier or feeder line is faulty.
- Distinguish an upstream path problem from a downstream one.
- Isolate an ingress noise problem from a plant equipment problem.

How to Configure Flap List Troubleshooting

This section describes how to configure the flap list operation on the Cisco CMTS. You can use either the command-line interface (CLI) commands or Simple Network Management Protocol (SNMP) commands to configure the flap list, to remove a cable modem from the list, or to clear the flap-list counters.

Configuring Flap List Operation Using the CLI (optional)

To configure the operation of the flap list, use the following procedure, beginning in EXEC mode. This procedure is optional, unless you want to change the default values for the flap list.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable flap-list insertion-time** *seconds* **Example:** `Router(config)# cable flap-list insertion-time 3600`	(Optional) Specifies the minimum insertion (registration) time interval in seconds. Any cable modem that makes a registration request more frequently than this period of time is placed in the flap list.
Step 4	**cable flap-list power-adjust threshold** *db* **Example:** `Router(config)# cable flap-list power-adjust threshold 5`	(Optional) Specifies the minimum power adjustment, in dB, that constitutes a flap-list event. **Note** A threshold of less than 2 dB can cause excessive flap-list event recording. If you need to change this parameter from its default, Cisco recommends setting it to 3 dB or higher.
Step 5	**cable flap-list miss-threshold** *misses* **Example:** `Router(config)# cable flap-list miss-threshold 10`	(Optional) Specifies the number of MAC-layer station maintenance (keepalive) messages that can be missed in succession before the CMTS places the cable modem in the flap list. **Note** A high miss rate indicates potential plant problems, such as intermittent upstream problems, fiber laser clipping, or common-path distortion.

	Command or Action	Purpose
Step 6	**cable flap-list aging** *minutes* **Example:** `Router(config)# cable flap-list aging 20160`	(Optional) Specifies how long, in minutes, the Cisco CMTS should keep information for cable modems in the flap list.
Step 7	**cable flap-list size** *number* **Example:** `Router(config)# cable flap-list size 4000`	Specifies the maximum number of cable modems that can be kept in the flap list. **Tip** To avoid wasting processor memory, do not set this value beyond the actual number of cable modems being serviced by the Cisco CMTS.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Clearing the Flap List and Counters Using the CLI (optional)

To clear one or more cable modems from the flap list, or to clear the flap list counters for one or more cable modems (while still keeping the modems in the flap list), use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear cable flap-list** *mac-addr* | **all**} [**save-counters**] **Example:** `Router# clear cable flap-list 0102.0304.0506 save-counters` **Example:** `Router# clear cable flap-list 000C.0102.0304`	Clears one or all cable modems from the flap list.

	Command or Action	Purpose
Step 3	**clear cable modem** {*mac-addr* | *ip-addr* | [**cable** *interface*] **all** | **oui***string* | **reject**} } **counters** **Example:** `Router# clear cable modem 172.12.23.45 counters` **Example:** `Router# clear cable modem oui Cisco counters` **Example:** `Router# clear cable modem reject counters` **Example:** `Router# clear cable modem c4/0 counters` **Example:**	Sets the flap-list counters to zero for one or more CMs.

Enabling or Disabling Power Adjustment Using the CLI (optional)

The Cisco CMTS can automatically monitor a cable modem's power adjustments and determine whether a particular cable modem requires a chance in the power adjustment method. To enable a cable interface to make automatic power adjustments, and to set the frequency threshold for when those adjustments are made, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0`	Enters cable interface configuration mode for the specified cable interface.
Step 4	**cable upstream** *n* **power-adjust** {**continue** *pwr-level* | **noise** *perc-pwr-adj* | **threshold value**} **Example:** `Router(config-if)# cable upstream 0 power-adjust threshold 2` **Example:** `Router(config-if)# cable upstream 0 power-adjust noise 50`	Enables automatic power adjustment on an upstream port for this cable interface. **Note** Repeat 4 for each upstream port on the cable interface.
Step 5	**cable upstream** *n* **freq-adj averaging** *percent* **Example:** `Router(config-if)# cable upstream 0 freq-adj averaging 50`	Specifies the percentage of frequency adjustment packets needed to change the adjustment method from the regular power-adjustment method to the automatic power adjustment method.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Caution The default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend that you adjust values. Cisco does recommend, however, that you clean up your cable plant should you encounter flapping cable modems.

Note In some instances, you might adjust certain values for the **cable upstream power-adjust** command: If CMs cannot complete ranging because they have reached maximum power levels, increase the **continue** *pwr-level* parameter beyond the default value of 2 dB. Values larger than 10 dB on "C" versions of cable interface line cards, or 5 dB on FPGA versions, are not recommended. If the flap list shows CMs with a large number of power adjustments, but the CMs are not detected as "noisy," decrease the **noise** *perc-pwr-adj* value. If too many CMs are unnecessarily detected as "noisy," increase the percentage.

Configuring Flap List Operation Using SNMP (optional)

To configure the Flap List Troubleshooting feature on the Cisco CMTS using SNMP, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists each of the configurable attributes:

Table 199: Flap-List Configuration Attributes

Attribute	Type	Range	Description
ccsFlapListMaxSize	Integer32	1 to 65536[145]	The maximum number of modems that a flap list can support per line card. The default is 100.[146]
ccsFlapListCurrentSize	Integer32	1 to 65536	The current number of modems in the flap list.[147]
ccsFlapAging	Integer32	1 to 86400	The flap entry aging threshold in minutes. The default is 10080 minutes (180 hours or 7 days).
ccsFlapInsertionTime	Integer32	60 to 86400	The worst-case insertion time, in seconds. If a cable modem has not completed the registration stage within this interval, the cable modem is inserted into the flap list. The default value is 90 seconds.
ccsFlapPowerAdjustThreshold	Integer32	1 to 10	When the power of the modem is adjusted beyond the power adjust threshold, the modem is inserted into the flap list.
ccsFlapMissThreshold	Unsigned32	1 to 12	When a cable modem does not acknowledge this number of consecutive MAC-layer station maintenance (keepalive) messages, the cable modem is placed in the flap list.

145 The allowable range when using SNMP for these parameters is 1 to 65536 (a 32-bit value), but the valid operational range is 1 to 8191.

146 This value is the same as set by the **cable flap-list size** command and is applied only to the command output. The flap list entries displayed via SNMP are not affected by this.

147 The number of SNMP entries is the same as this value. The number of the CLI entries depends on the value set by **ccsFlapListMaxSize**.

Note **ccsFlapListMaxSize** controls the display of the flap list per downstream cable interface. As long as the number of flap list entries per line card does not exceed 8191, these entries will be stored in the system, and will not be displayed via CLI.

ccsFlapListCurrentSize reflects the number of flap list entries of all the line cards that in the system, regardless of their visibility to the CLI.

Clearing the Flap List and Counters Using SNMP (optional)

To remove a cable modem from the flap list or to clear one or all of the flap-list counters, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists the attributes that clear the SNMP counters.

Table 200: Attributes to Clear the Flap List

Attribute	Type	Description
ccsFlapResetAll	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapClearAll	Boolean	Setting this object to True (1) removes all cable modems from the flap list, and destroys all entries in the ccsFlapTable. If a modem keeps flapping, the modem is added again into the flap list as a new entry.

Note The ccsFlapLastClearTime attribute contains the date and time that the entries in the ccsFlapTable table were last cleared.

How to Monitor and Troubleshoot Using Flap Lists

Displaying the Flap List Using the show cable flap-list Command

To display the current contents of the flap list, use the show cable flap-list command in privileged EXEC mode. This command has the following syntax:

- **show cable flap-list—**Displays the complete flap list.

- **show cable flap-list sort-interface—**Displays the complete flap list sorted by cable interface.
- **show cable flap-list cable** *interface* **upstream** *port***—**Displays the flap list for a specific cable interface, or for a specific upstream port on that cable interface.

To change the way the output is sorted, add one of the following optional keywords:

- **sort-flap—**Sorts the output by the number of times that the cable modem has flapped.
- **sort-time—**Sorts the output by the most recent time that the cable modem flapped.

The following example shows typical output of the **show cable flap-list** command.

```
Router# show cable flap-list
Mac Addr       CableIF Ins    Hit   Miss    CRC  P-Adj   Flap    Time
0010.9500.461f C1/0 U1 56  18857    887      0      1    116 Jun 1  14:09:12
0010.9500.446e C1/0 U1 38  18686   2935      0      1     80 Jun 2  19:03:57
0010.9500.38ec C1/0 U2 63  18932   1040      0      8    138 Jun 2  23:50:53
0010.9500.4474 C1/0 U2 65  18913   1053      0      3    137 Jun 2  09:30:09
0010.9500.4672 C1/0 U2 56  18990   2327      0      6    124 Jun 2  10:44:14
0010.9500.38f0 C1/0 U2 50  18964   2083      0      5    111 Jun 2  20:46:56
0010.9500.e8cb C1/0 U2  0   6537    183      0      1      5 Jun 2  22:35:48
0010.9500.38f6 C1/0 U3 50  19016   2511      0      2    104 Jun 2  07:46:31
0010.9500.4671 C1/0 U3 43  18755   3212      1      1     89 Jun 1  19:36:20
0010.9500.38eb C1/0 U0 57  36133   1608      0      6    126 Jun 2  20:04:58
0010.9500.3ce2 C1/0 U0 44  35315   1907      0      4     99 Jun 2  16:42:47
0010.9500.e8d0 C1/0 U2  0  13213    246      0      1      5 Jun 3  04:15:30
0010.9500.4674 C1/0 U2 56  36037   2379      0      4    121 Jun 3  00:34:12
0010.9500.4677 C1/0 U2 40  35781   2381      0      4     91 Jun 2  12:14:38
0010.9500.4614 C1/0 U2 40  21810   2362      0    502    586 Jun 2  21:43:02
0010.9500.3be9 C1/0 U2 63  22862    969      0      0    128 Jun 1  14:09:03
0010.9500.4609 C1/0 U2 55  22723   2127      0      0    112 Jun 1  14:08:02
0010.9500.3cb8 C1/0 U2 49  22607   1378      0      0    102 Jun 1  14:08:58
0010.9500.460d C1/0 U3 46  22477   2967      0      2     96 Jun 2  17:03:48
0010.9500.3cba C1/0 U3 39  22343   3058      0      0     81 Jun 1  14:13:16
0010.9500.3cb4 C1/0 U3 38  22238   2936      0      0     79 Jun 1  14:09:26
0010.9500.4612 C1/0 U3 38  22306   2928      0      0     79 Jun 1  14:09:29
Router#
```

Displaying the Flap List Using the show cable modem flap Command

To display the contents of the flap list for a specific cable modem, use the **show cable modem flap** command in privileged EXEC mode. This command has the following syntax:

- **show cable modem** [*ip-address* | *mac-address*] **flap—**Displays the flap list for a specific cable modem, as identified by its IP address or MAC address.
- **show cable modem cable***interface* [**upstream** *port*] **flap—**Displays the flap list for all cable modems on a specific cable interface.

Note The **show cable modem flap** command displays information similar to that shown by the **show cable flap-list** command, except it displays this information on a per-modem basis.

The following example shows sample output for the **show cable modem flap** command for a particular cable modem:

```
Router# show cable modem 0010.7bb3.fcd1 flap
MAC Address    I/F       Ins   Hit   Miss  CRC   P-Adj   Flap  Time
```

```
0010.7bb3.fcd1 C5/0/U5   0     36278 92    0     369     372   Jun 1  13:05:23 (18000msec)
```

The following example shows sample output for the **show cable modem flap** command for all cable modems on a specific cable interface:

```
Router# show cable modem cable 6/0/0 flap
MAC Address    I/F           Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0025.2e34.4386 C6/0/0/U0     0     46778 3980  0      0      0     (14212 msec)
0025.2e2f.d4b6 C6/0/0/U0     0     48002 1899  0      0      0     (18000 msec)
0025.2e2f.d4de C6/0/0/U0     0     48098 1889  0      0      0     (19552 msec)
0023.bee1.e96b C6/0/0/U0     0     46658 4351  0      0      0     (22432 msec)
0025.2e2f.d4d8 C6/0/0/U0     0     21979 781   0      0      0     ( -- )
0025.2e2f.d48c C6/0/0/U0     0     48048 1835  0      0      0     ( -- )
0025.2e2f.d490 C6/0/0/U0     0     48029 1819  0      0      0     ( -- )
```

Displaying the Flap List Using SNMP

To display the contents of the flap list using SNMP, query the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB. This table contains an entry for each cable modem. the table briefly describes each attribute in this table.

Table 201: cssFlapTable Attributes

Attribute	Type	Description
cssFlapMacAddr	MacAddress	MAC address of the cable modem's cable interface. Identifies a flap-list entry for a flapping cable modem.
ccsFlapUpstreamIfIndex	InterfaceIndex	Upstream being used by the flapping cable modem.
ccsFlapDownstreamIfIndex	InterfaceIndex	Downstream being used by the flapping cable modem.
ccsFlapLastFlapTime	DateAndTime	Time stamp for the last time the cable modem flapped.
ccsFlapCreateTime	DateAndTime	Time stamp that this entry was added to the table.
ccsFlapRowStatus	RowStatus	Control attribute for the status of this entry.

Attribute	Type	Description
ccsFlapInsertionFailNum	Unsigned32	Number of times the CM comes up and inserts itself into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the **cable flap-list insertion-time** command or ccsFlapInsertionTime attribute. When the cable modem cannot finish registration within the insertion time (ccsFlapInsertionTime), it resends the Initial Maintenance packet. When the CMTS receives the packet sooner than expected, the CMTS increments this counter.
ccsFlapHitNum	Unsigned32	Number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds.)
ccsFlapMissNum	Unsigned32	Number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. If the CMTS misses a ranging request within 25 msec, then the miss number is incremented.
ccsFlapCrcErrorNum	Unsigned32	Number of times the CMTS upstream receiver flagged a packet with a CRC error. A high value indicates that the cable upstream may have a high noise level. The modem may not be flapping yet, but this could become a possible problem.
ccsFlapPowerAdjustmentNum	Unsigned32	Number of times the cable modem upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power-adjustment threshold, the number is incremented.

Attribute	Type	Description
ccsFlapTotalNum	Unsigned32	Number of times a modem has flapped, which is the sum of the following: • When ccsFlapInsertionFailNum is increased • When the CMTS receives a miss followed by a hit • When ccsFlapPowerAdjustmentNum is increased
ccsFlapResetNow	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapLastResetTime	DateAndTime	Time stamp for when all the counters for this particular entry were reset to zero.

Displaying Flap-List Information for Specific Cable Modems

To use SNMP requests to display flap-list information for a specific cable modem, use the cable modem's MAC address as the index to retrieve entries from the ccsFlapTable. Use the following procedure to retrieve flap-list entries for a particular cable modem.

Step 1 Convert the cable modem's MAC address into a dotted decimal string. For example, the MAC address 000C.64ff.eb95 would become 0.12.100.255.235.149.

Step 2 Use the dotted decimal version of the MAC address as the instance for requesting information from the ccsFlapTable. For example, to retrieve the ccsFlapHits, ccsFlapMisses, and ccsFlapPowerAdjustments values for this cable modem, you would make an SNMP request for the following objects:

- ccsFlapHits.0.12.100.255.235.149
- ccsFlapMisses.0.12.100.255.235.149
- ccsFlapPowerAdjustments.0.12.100.255.235.149

Example

Assume that you want to retrieve the same flap-list information as the **show cable flap-list** command for a cable modem with the MAC address of 000C.64ff.eb95:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
000C.64ff.eb95  Cable3/0/U4  3314  55605 50460 0    *42175 47533 Jan 27 02:49:10
```

```
Router#
```

Use an SNMP tool to retrieve the ccsFlapTable and filter it by the decimal MAC address. For example, using the standard Unix **getone** command, you would give the following command:

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149

ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4  01 1b   02 33  1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4  01 16   03 23  22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4  01 16   03 20  18 00
csh%
```

To request just one particular value, use the decimal MAC address as the instance for that object:

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149

ccsFlapMisses.0.12.100.255.235.149 = 50736
csh %
```

Troubleshooting Suggestions

This section provides tips on how to interpret the flap-list counters, as well as how to determine the optimum power level for a flapping cable modem.

Troubleshooting Tips

This section includes suggestions on how to interpret different network conditions based on the flap-list statistics:

- Condition 1: Low miss or hit ratio (< 2 percent for a Cisco uBR-MC16 card), low insertion, low P-Adj, low flap counter, and old time stamp. Analysis: This exhibits an optimal network situation.
- Condition 2: High ratio of misses over hits (> 10 percent). Analysis: Hit and miss analysis should be done after the Ins count stops incrementing. In general, if the hit and miss counts are about the same order of magnitude, the upstream can be experiencing noise. If the miss count is greater, then the modem is probably dropping out frequently and not completing registration. The upstream or downstream might not be stable enough for reliable link establishment. Very low hits and miss counters and high insertion counters indicate provisioning problems.
- Condition 3: Relatively high power-adjustment counter. Analysis: Indicates that the power-adjustment threshold is probably set at default value of 2 dB. The modem transmitter step size is 1.5 dB, but the headend can command 0.25 dB step sizes. Tuning your power threshold to 6 dB is recommended to decrease irrelevant entries in the flap list. The power-adjustment threshold can be set using cable flap

power threshold <0-10 dB> in the Cisco IOS global configuration mode. A properly operating HFC network with short amplifier cascades can use a 2 to 3 dB threshold.

- Condition 4: High P-Adj and CRC errors. Analysis: This condition can indicate that the fiber node is clipping the upstream return laser. Evaluate the modems with the highest CRC count first. If the modems are not going offline (Ins = 0), this is not noticed by subscribers. However, they could receive slower service due to dropped IP packets in the upstream. This condition also results in input errors on the Cisco CMTS router cable interface.
- Condition 5: High insertion rate. Analysis: If link reestablishment happens too frequently, the modem is usually having a registration problem. This is indicated by a high Ins counter, which tracks the Flap counter.

Performing Amplitude Averaging

The CMTS uses an averaging algorithm to determine the optimum power level for a cable modem with low carrier-to-noise ratio that is making excessive power adjustments—known as flapping. To avoid dropping flapping cable modems, the CMTS averages a configurable number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the CMTS maintains connectivity with affected cable modems. You can interpret these power adjustments, however, as indicating unstable return path connections.

The **show cable flap-list** and **show cable modem** commands are expanded to indicate to which paths the CMTS is making power adjustments and which modems have reached maximum transmit power settings. These conditions indicate unstable paths that should be serviced.

The following example shows the output of the **show cable flap-list** command:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
 0010.7bb3.fd19  Cable1/0/U1  0     2792  281   0    *45    58    Jul 27 16:54:50
 0010.7bb3.fcfc  Cable1/0/U1  0     19    4     0    !43    43    Jul 27 16:55:01
 0010.7bb3.fcdd  Cable1/0/U1  0     19    4     0    *3     3     Jul 27 16:55:01
```

The asterisk (*) indicates that the CMTS is using the power-adjustment method on this modem. An exclamation point (!) indicates that the modem has reached maximum transmit power.

Output of the **show cable modem** command appears below:

```
Router# show cable modem
 Interface   Prim Online     Timing Rec    QoS CPE IP address      MAC address
             Sid  State      Offset Power
 Cable1/0/U0 1    online     2257    0.00  3   0   10.30.128.142   0090.8330.0217
 Cable1/0/U0 2    online     2262  *-0.50  3   0   10.30.128.145   0090.8330.020f
 Cable1/0/U0 3    online     2260    0.25  3   0   10.30.128.146   0090.8330.0211
 Cable1/0/U0 4    online     2256   *0.75  3   0   10.30.128.143   0090.8330.0216
 Cable1/0/U0 5    online     2265   *0.50  3   0   10.30.128.140   0090.8330.0214
 Cable1/0/U0 6    online     2256    0.00  3   0   10.30.128.141   0090.8330.0215
 Cable1/0/U0 7    online     4138  !-1.00  3   1   10.30.128.182   0050.7366.124d
 Cable1/0/U0 8    online     4142  !-3.25  3   1   10.30.128.164   0050.7366.1245
 Cable1/0/U0 9    online     4141  !-3.00  3   1   10.30.128.185   0050.7366.17e3
 Cable1/0/U0 10   online     4142  !-2.75  3   0   10.30.128.181   0050.7366.17ab
 Cable1/0/U0 11   online     4142  !-3.25  3   1   10.30.128.169   0050.7366.17ef
```

Similar to the **show cable flap-list** command display, the * symbol in the **show cable modem** command output indicates that the CMTS is using the power-adjustment method on this CM. The ! symbol indicates that the CM has reached maximum transmit power.

Using Other Related Commands

The following related Cisco IOS commands can be used to do maintenance on or display information about a cable modem.

- The following clears the counters for a cable modem (or all cable modems) in the station maintenance list:

```
clear cable modem {mac-addr | ip-addr | all} counters
```

- The following displays the QoS, modem status, In and Out octets, IP and MAC addresses per SID:

```
show int cable slot/port sid
```

- The following drops the modem's RF link by removing a modem from the keepalive polling list. This forces the modem to reset. Note the warning below.

```
clear cable-modem {mac-addr | ip-addr | all} reset
```

Tip The **clear cable-modem** *all* **reset** command causes all modems to go offline and disrupt service for your users. It is best used in a test or nonproduction environment.

- The following uses a MAC-layer ping to determine if the cable modem is online. It uses smaller data units on the wire than a standard IP ping, resulting in lower overhead. This command works even if the IP layer in the modem is down or has not completed registration:

```
ping DOCSIS cable-modem mac-addr | IP address
```

- The following displays the timing offset, receive power, and QoS values by cable interface, SID, and MAC address:

```
show cable modem [ip-address | MAC-address]
```

- The following displays the current allocation table and frequency assignments:

```
show cable spectrum-group [spectrum group number]
```

- The following displays maximum, average, and minimum percent of online time and offline time for a given SID on a given cable router interface:

```
show int slot/port sid connectivity
```

- The following command displays input and output rates, input errors, CRC, frames, overruns, underruns, collisions, interface resets. High input errors in the CMTS retrieved from this query suggest noisy upstream. In older versions of the chassis, loose midplane and line card screws caused a similar problem:

```
show interface slot/downstream-port
```

- The following command displays upstream packet discards, errors, error-free packets, correctable and uncorrectable errors, noise, and micro-reflection statistics.

```
show interface slot/downstream-port upstream
```

Configuration Examples for Flap List Troubleshooting

The following excerpt from a configuration file shows a typical flap-list configuration:

```
!
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 3
cable flap-list miss-threshold 4
cable flap-list aging 8
cable flap-list size 8191
...
```

Additional References

For additional information related to the Flap List Troubleshooting feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco CMTS Cable Command Reference
Cisco Broadband Troubleshooter	http://www.cisco.com/c/en/us/support/cloud-systems-management/broadband-troubleshooter/tsd-products-support-series-home.html

Standards

Standards[148]	Title
ANSI/SCTE 22-1 2012 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification

Standards[148]	Title
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification

148 Not all supported standards are listed.

MIBs

MIBs[149]	MIBs Link
CISCO-CABLE-SPECTRUM-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

149 Not all supported MIBs are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	To locate and download Request for Comments (RFCs) and Internet Drafts, see the Internet Engineering Task Force (IETF) web site at the following URL: http://www.ietf.org/index.html

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Flap List Troubleshooting

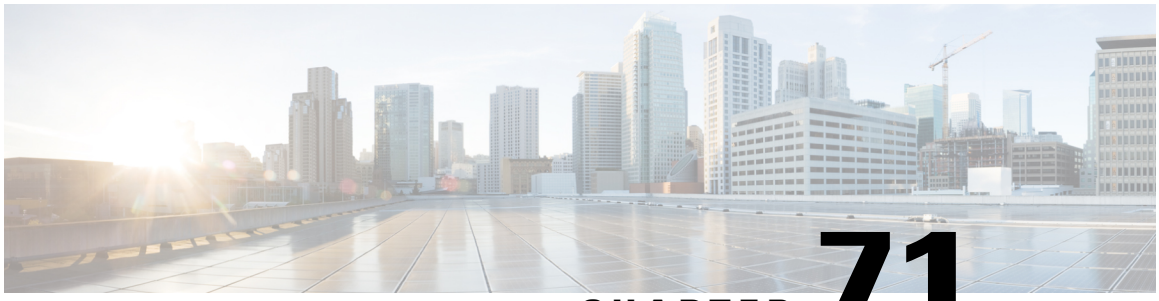
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 202: Feature Information for Flap List Troubleshooting

Releases	Feature Information
Release 11.3 NA	This feature was introduced on the Cisco uBR7200 series routers.
Release 12.0(4)XA	The *days* parameter was removed from the **cable flap-list aging** command.
Release 12.0(7)XR, 12.1(2)EC	The output of **show cable flap-list** command was enhanced to show when the Cisco uBR7200 series router has detected an unstable return path for a particular CM and has made an automated power adjustment.
Release 12.1(5)EC	This feature was supported on the Cisco uBR7100 series routers.
Release 12.1(7)CX	The ccsFlapClearAll attribute was added to the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB MIB.
12.2(4)BC1	This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms. The **show cable modem flap** command was also introduced to display flap-list information for individual cable modems.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.	



CHAPTER 71

IPDR Streaming Protocol on the Cisco CMTS Routers

First Published: December 17, 2008

Last Updated: July 11, 2012

The Cisco universal broadband router supports the Internet Protocol Detail Record (IPDR) streaming protocol feature that provides high volume data exported from the network equipment to mediation systems such as the Operations Support Systems (OSS) or Business Support Systems (BSS). IPDR provides information about IP-based service usage and other activities that are used by OSS and BSS. This protocol provides a mechanism to collect data from various network elements or equipment using a push model as opposed to the conventional Simple Network Management Protocol (SNMP) polling mechanism.

Based on the DOCSIS 3.0 specifications, the IPDR feature optimizes time and resource efficiency in the transfer of large amounts of performance metrics to the management systems. DOCSIS 3.0 introduces five management features or the FCAPS model. FCAPS represents Fault, Configuration, Accounting, Performance and Security.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Configuring IPDR Streaming Protocol

The table shows the hardware compatibility prerequisites for the IPDR streaming protocol.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 203: Cable Hardware Compatibility Matrix for the IPDR Streaming Protocol

Cisco CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later • PRE2 • PRE4 • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [150]
Cisco uBR7246VXR Universal Broadband Routers	Cisco IOS Release 12.2(33)SCD and later • Network Processing Engine G2 (NPE-G2)	Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [151]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later • NPE-G2	Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

150 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

151 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Configuring IPDR Streaming Protocol

- An IPDR exporter can be connected to many collectors, but it will only send data to the highest priority operating collector at any given time.
- Each IPDR session can be associated to one active (zero) or more standby collector with priority.

Information About IPDR Streaming Protocol

IPDR Streaming Protocol is designed to address the need for a reliable, fast, efficient, and flexible export process of high volume data records such as billing, performance and diagnostic data.

The IPDR/SP process communicates with IPDR collectors. The IPDR streaming protocol supports multiple IPDR sessions. The architecture supports primary and secondary collectors for failover purposes. At any time, data is sent to only one collector. If the exporter to primary collector connection fails due to any reason, the data is sent to the secondary collector. Depending on the network configuration, you can have only one primary collector for each session, while for different sessions, you can have different primary collectors. For example, there may be a billing collector, a diagnostic collector, and so on.

Note IPDR exporter refers to the Cable Modem Termination System (CMTS) and the IPDR collector refers to the network equipment.

Data Collection Methodologies

IPDR is the data generated or collected for various performance related metrics such as billing information, diagnostics, network topology, signal quality monitoring, and other management data. These data are based on the FCAPS model (Fault, Configuration, Accounting, Performance and Security.)

The IPDR client application communicates with the IPDR exporter using the IPDR_GET_SESSIONS message to identify the streams provided by the exporter, and the exporter sends responses to the client using the IPDR_GET_SESSIONS_RESPONSE message. This data collection method is based on the *Operations Support System Interface Specification* (CM-SP-OSSIv3.0-I13-101008).

Beginning with Cisco IOS Release 12.2(33)SCE, the IPDR_GET_SESSIONS_RESPONSE message includes the SessionBlock.reserved attribute to identify the IPDR session ID. This attribute helps the Cisco CMTS router define an IPDR session ID for each data collection mechanism supported for each IPDR service definition. This attribute was not used in Cisco IOS Releases earlier to Cisco IOS Release 12.2(33)SCE.

Note You must use a Cisco CMTS router running Cisco IOS Release 12.2(33)SCE or later, if your IPDR client application looks for the SessionBlock.reserved attribute in the IPDR_GET_SESSIONS_RESPONSE message.

The IPDR feature defines methods for the collectors or network elements to collect data from the CMTS. Below is the list of collection methodologies:

Time Interval Session: In this method, the CMTS follows a schedule-based session to stream data at a periodic time interval. A time interval is the time gap between two adjacent sessions' start messages. This method is

managed by the CMTS in controlling the start and stop operation of a session. The time interval session terminates after the CMTS exports the records.

Note During the course of a one-time interval when the CMTS is streaming records, if another time interval is expected, the CMTS will ignore the new time interval and continue exporting the data until the previous time interval ends.

Event-based Session: In this method, the CMTS can export records at any time, when the session is open. In other words, this method works on an open-ended session.

Ad-hoc Session: In this method, the CMTS creates a session, allows data streaming, and closes the session when the data export is complete or when a closing command is generated.

A new session is created by issuing the **ipdr session** command. After, the CMTS receives the FLOW_START message from the collector, the CMTS exporter sends a SESSION_START message to start exporting the IPDR data from the collector. After all data is transported, the exporter receives a ACK message from the collector, and then sends a SESSION_STOP message to the collector. This method is known as the Ad-hoc session.

IPDR Access Control List

The IPDR streaming protocol in Cisco uBR10012 router is enhanced to improve the security of the IPDR collector function. This enhancement prevents the validation and authentication of the fake IPDR collectors, thus preventing billing theft.

This enhancement is optional and may be enabled or disabled. To enable the IPDR Access Control List enhancement, use the **ipdr authorization** command. Effective with Cisco IOS Release 12.2(33)SCI2, only the IPDR collectors on the CMTS network side are authorized based on the authorization procedure.

The **ipdr collector** command is enhanced to configure a NAT address for an IPDR collector that operates from a NAT router. For authorization of such IPDR collectors, the NAT address is also configured for the IPDR collectors using the **nat-address** keyword.

Restrictions

The following restrictions are applicable when the IPDR Access Control List enhancement is enabled:

- Effective with Cisco IOS Release 12.2(33)SCI2, the IPDR collectors on the CMTS bundle side are blocked. This block is irrespective of whether the **ipdr authorization** is enabled or not.
- An IPDR collector that operates from within a NAT router, the NAT address parameter may be configured for that IPDR collector.
- For authentication:
  - If the IPDR collector operates from within a NAT router, then the NAT address of the IPDR collector must match the NAT address of the listed IPDR collector. The IP address of the IPDR collector also must match the IP address of the listed IPDR collector.
  - If the IPDR collector does not operate from within a NAT router, only the IP address of the IPDR collector must match the IP address of the listed IPDR collector.

How to Configure IPDR Streaming Protocol

This section describes the configuration tasks that are performed when using the IPDR streaming protocol feature on the Cisco CMTS platforms.

Note Use no ipdr command to remove the IPDR configuration.

Configuring the IPDR Session

To enable the CMTS application to add a session to the IPDR exporter, use the ipdr session command in global configuration mode.

Use the no form of the command to remove the IPDR session.

Note
- The session ID must be unique.
- To remove an active session, you must deactivate it before removing it.

>

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	ipdr session session_id session_name session_descr **Example:** `Router(config)# ipdr session 1 samis_sxn test`	Enables the CMTS application to add a session to the IPDR exporter.

Configuring the IPDR Type

To configure the IPDR session type, use the ipdr type command in global configuration mode. The IPDR session types that can be defined using this command are event type, time-interval type, and the ad hoc type.

Use the no form of the command to reset the session type to the default "event" type.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	ipdr type session_id [ad-hoc | event | time-interval value] **Example:** `Router(config)# ipdr type 1 time-interval 15`	Enables the CMTS application to configure an IPDR session type.

What to Do Next

Note Once the IPDR session type is configured, only the templates supported by this IPDR type are allowed be associated with it. Also, the console provides information about those templates that are not supported by this IPDR session type when the type is changed.

Configuring the IPDR Collector

To configure the IPDR collector details, use the ipdr collector command in global configuration mode. The port number is used when an exporter creates an active connection.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr collector** **Example:** `Router(config)# ipdr collector federal 192.168.6.5`	Enables the CMTS application to configure an IPDR collector and authenticate the IPDR protocol. **Note** Configure the NAT address in case of an IPDR collector that is operating in a NAT enabled network.

Configuring the IPDR Associate

To associate the collector with a session, use the ipdr associate command in global configuration mode.

Before You Begin

- You must deactivate the session before configuring the associate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr associate session_id collector_name priority** **Example:** `Router(config)# ipdr associate 1 federal 1`	Associates the collector with a session.

Configuring the IPDR Template

To add an IPDR template to the IPDR session, use the ipdr template command in global configuration mode. The template list can be viewed by entering a "?" at the command prompt.

Note
- You can add only the system-supported templates.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr template session_id template_name** **Example:** `Router(config)# ipdr template 1 SAMIS`	Adds an IPDR template to the IPDR session.

Configuring the IPDR Exporter

Starting with Cisco IOS Release 12.2(33)SCG, IPDR exporter parameters such as keepalive timer count, the maximum number of unacknowledged records, and unacknowledged timeout interval value can be configured using the following commands.

- **ipdr exporter keepalive—**Sets the keepalive timer count value on the IPDR Exporter.
- **ipdr exporter max-unacked—**Sets the maximum number of unacknowledged records on the IPDR Exporter.
- **ipdr exporter ack-timeout—**Sets the time interval for acknowledged records on the IPDR Exporter.

Note Starting Cisco IOS Release 12.2(33)SCE, the default value for DataAckTimeInterval is 60 seconds and the default value for DataAckSequenceInterval is 200 seconds.

You can set the values for the IPDR parameters to customize exporter for the collectors used in the facility. However, these commands are optional, so if not configured, the default values of the commands are used when **ipdr exporter start** command is executed.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr exporter keepalive** *time_interval* **Example:** `Router(config)# ipdr exporter keepalive 300`	(Optional) Sets the keepalive timer count for the IPDR Exporter. The valid range is from 5 to 300 seconds. The default value is 300.
Step 4	**ipdr exporter max-unacked** *records* **Example:** `Router(config)# ipdr exporter max-unacked 200`	(Optional) Sets the number of maximum unacknowledged records on the IPDR Exporter. The valid range is from 5 to 200 records. The default value is 200.
Step 5	**ipdr exporter ack-timeout** *time_interval* **Example:** `Router(config)# ipdr exporter ack-timeout 60`	(Optional) Sets the acknowledged records timeout interval on the IPDR Exporter. The valid range is from 5 to 60 seconds. The default value is 60.
Step 6	ipdr exporter start **Example:** `Router(config)# ipdr exporter start`	Enables the CMTS application to start the IPDR exporter process to connect the exporter and the collector.

Configuration Examples for IPDR Streaming Protocol

Example: Configuring the IPDR Session

The following example shows how to configure the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr session 1 test no_descr
```

Example: Configuring the IPDR Type

The following example shows how to configure the IPDR “time-interval” session type for a time interval of 15 minutes.

```
Router> enable
Router# configure terminal
Router(config)# ipdr type 1 time-interval 15
```

Example: Configuring the IPDR Collector

The following example shows how to configure the IPDR collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr collector federal 209.165.200.225
```

Example for Configuring the IPDR Collector with NAT Address

Effective with Cisco IOS Release 12.2(33)SCI2, this example shows the **nat-address** keyword used to configure the NAT address for an IPDR collector:

```
Router(config)#ipdr collector federal 192.0.2.225 nat-address 192.0.2.51
```

Example: Configuring the IPDR Associate

The following example shows how to associate the collector with a session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr associate 1 federal 1
```

Example: Configuring the IPDR Template

The following example shows how to add an IPDR template to the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr template 1 SAMIS-TYPE1
```

Example: Configuring the IPDR Exporter

The following example shows how to configure the IPDR exporter process to connect the exporter and the collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr exporter keepalive 300
Router(config)# ipdr exporter max-unacked 200
Router(config)# ipdr exporter ack_timeout 60
Router(config)# ipdr exporter start
```

Example: Configuring the IPDR Authorization

The following example shows how to configure the IPDR authorization.

```
Router> enable
Router# configure terminal
Router(config)# ipdr authorization
```

Verifying IPDR Streaming Protocol

This section describes the commands used for verification of the IPDR streaming protocol feature on the Cisco CMTS platforms.

Verifying the IPDR Collector

The **show ipdr collector** command displays the collector information, message statistics, and event for all the sessions that are associated with the collector.

The following example shows the sample output for the **show ipdr collector** command.

```
Router# show ipdr collector federal
Collector Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:28:22 Collector in session 1 Statistics:
 Transmitted 12658 Acknowledged 12658 Enqueued 12658 Lost 0
 Last Event: Event Id 1 IPDR_EVENT_SERVER_CONNECTED - INCOMING
Router(config)#
```

Verifying IPDR exporter

The **show ipdr exporter** command displays information about the IPDR Exporter state as listed below.

- started
- not started
- not initialized

The following example shows the sample output for the **show ipdr exporter** command:

```
Router# show ipdr exporter
IPDR exporter is started.
Current parameters:
```

```
        KeepAliveInterval   :300
        AckTimeInterval     :60
        AckSequenceInterval :200
Router#
```

Verifying IPDR session

The **show ipdr session** command displays the session details such as the session ID, description, and the session state for all sessions as well as for a specific session.

The following example shows the sample output for the **all** keyword for the **show ipdr session** command.

```
Router# show ipdr session all
Session ID: 1, Name: utilsta, Descr: test, Started: False
```

The following example shows the sample output for the **session_id** keyword for the **show ipdr session** command.

```
Router# show ipdr session 1
Session ID: 1, Name: utilsta, Descr: test, Started: False
2001-07-05T19:36:28 Statistics:
Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
Name: federal, IPAddr: 192.0.2.0, Port: 0, Priority: 1
```

Verifying IPDR Session Collector

The **show ipdr session collector** command displays the details of a collector that is associated with a specific session. Because there can be multiple collectors associated to a session, this command is used to show a specific session-collector pair.

The following example shows the sample output for the **show ipdr session collector** command.

```
Router# show ipdr session 1 collector federal
Session ID: 1, Name: utilsta, Descr: test, Started: False
Collecotr Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:38:02 Collector in session 1 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 Last Event: Event Id 0 WRONG_EVENT_ID
```

Verifying IPDR Session Template

The **show ipdr session template** command displays the list of all active templates supported by a specific session.

The following example shows the sample output for the **show ipdr session template** command.

```
Router# show ipdr session 1 template
Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CMSERVICE-FLOW-TYPE,
Type: DOCSIS-Type, KeyNumber: 22
Session 1 has totally 1 templates.
```

Additional References

The following sections provide references related to configuring the IPDR streaming protocol feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_release_notes_list.html
IPDR/SP 2.1	IPDR/SP Protocol Specification Version 2.1 http://www.ipdr.org

Standards

Standard	Title
DOCSIS 3.0 OSSI	Data-Over-Cable Service Interface Specifications DOCSIS 3.0 Operations Support System Interface Specification CM-SP-OSSIv3.0-I13-101008 http://www.cablelabs.com

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1014 XDR	XDR: External Data Representation Standard

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

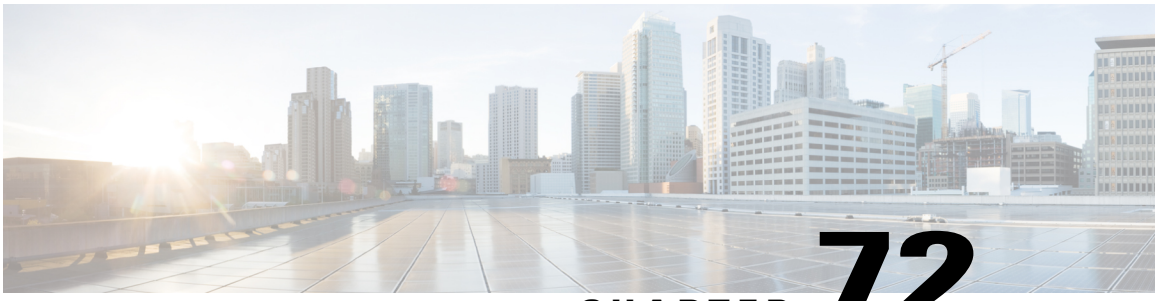
Feature Information for IPDR Streaming Protocol

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 204: Feature Information for IPDR Streaming Protocol

Feature Name	Releases	Feature Information
IPDR Streaming Protocol	12.2(33)SCB	The Cisco universal broadband router supports the IPDR streaming protocol feature that enables efficient and reliable delivery of high volume data records from the service elements to any systems, such as mediation systems and BSS/OSS. The following sections provide information about this feature:
Data Collection Methodologies and DOCSIS 3.0 IPDR Schema	12.2(33)SCD2	This feature was introduced in this release. The following sections provide information about this feature: The following command was introduced: ipdr type
IPDR Exporter parameters such as keepalive timer value, maximum unacknowledged records, and acknowledged records timer value can be configured using the CLI.	12.2(33)SCG	The following commands were introduced: • **ipdr exporter keepalive** • **ipdr exporter max-unacked** • **ipdr exporter ack-timeout**
IPDR Access Control List	12.2(33)SCI2	This feature was introduced in this release. The following command was introduced: **ipdr authorization** The following command was modified: **ipdr collector**



CHAPTER 72

GOLD Health Monitoring for the Cisco UBR10012 Universal Broadband Router

First Published: November 16, 2009

Last Updated: November 29, 2010

Generic Online Diagnostic (GOLD) is a health monitoring feature implemented on the Cisco UBR10012 Universal Broadband Router in the Cisco IOS Release 12.2(33)SCC. The GOLD functionality is developed to provide online diagnostic capabilities that run at bootup, in the background on a periodic basis, or based on demand from the CLI.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for GOLD

The table shows the hardware and software compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 205: GOLD Support for the Cisco CMTS Routers Hardware and Software Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [152]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [153]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

152 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
153 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for GOLD feature

- GOLD test cases are designed on a per chip or per interface level and are not expected to monitor at a per modem or per service flow level.
- GOLD diagnostic test cases supported in the Cisco IOS Release 12.2(33)SCC are as follows:
  - Low Latency Queue (LLQ) Drop Monitor Test: Implemented on 5x20 cable line card (CLC) (Test520LLQDrops), 20x20 CLC (Test2020LLQDrops), and Modena (TestModenaLLQDrops).
  - Guardian Index Leak Test: Implemented only on 5x20 Guardian LC (TestBlazeIndexLeak).
  - CLC Memory Leak Test: Implemented on 5x20 and 20x20 LC (TestMemLeaks).

Information About GOLD

The following sections provide details of the GOLD feature:

Limitations of Existing Logging Mechanism

To provide high-availability for a router without any downtime it is imperative to analyze the stability of a system. The primary method of discovering the cause of system failure is system messages. However, there are certain system failures that do not send notifications. It is difficult to understand the cause of these system failures, as the existing logging mechanism fails to notify or maintain a log of these failures.

Understanding the Importance of GOLD Functionality

As there are certain system failures that do not send any notification or keep a log of failure, it is essential to address these limitations. The GOLD feature has been designed specifically to provide error detection by polling for errors for those system modules that do not have any notification mechanism. GOLD has been implemented on the Cisco UBR10012 router to actively poll for system errors. Online diagnostics is one of the requirements for high availability (HA). HA is a a set of quality standards that seeks to limit the impact of equipment failures on the network. A key part of HA is detecting system failures and taking corrective actions while the system is running in a live network.

Understanding the GOLD Feature

The GOLD feature is primarily used to poll for system errors targeted for those components, which do not send a notification upon failure. Although the infrastructure can be used to poll for both hardware and system errors, the main scope is to poll for status and error registers on physical hardware device. The Cisco UBR10012 Router uses a distributed GOLD implementation. In this model, the core Cisco IOS GOLD subsystem is linked on both the route processor (RP) and the cable line cards.

Diagnostic tests can be registered either as local tests which run on the RP or as proxy tests which run on the line cards. When a proxy test is requested on the RP, a command is sent using Inter-Process Communication (IPC) to the line card to instruct it to run the test locally. The results are then returned to the RP using IPC.

Tests are specified by card type on a per slot/subslot basis. Diagnostic tests can be run either on bootup, periodically (triggered by a timer), or on demand from the CLI. GOLD feature is managed through a range of commands which are mainly used to provide on-demand diagnostic tests, schedule tests at particular intervals, monitor the system health on periodic basis and to view the diagnostic test results.

Configuring Online Diagnostics

The following sections describe how to configure various types of diagnostics and view test reports:

Configuring the Bootup Diagnostics Level

You can configure the bootup diagnostics level as minimal or complete or you can bypass the bootup diagnostics entirely. Enter the **complete** keyword to run all bootup diagnostic tests and the **minimal** keyword to run minimal tests such as loopback. Enter the **no** form of the command to bypass all diagnostic tests. The default bootup diagnostics level is minimal.

Note None of the currently implemented tests on the Cisco UBR 10012 Router are bootup tests.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **diagnostic bootup level {minimal | complete}** **Example:** `Router(config)#` **diagnostic bootup level complete**	Configures the bootup diagnostic level.

Configuring On-Demand Diagnostics

You can run the on-demand diagnostic tests from the CLI. You can set the execution action to either stop or continue the test when a failure is detected or to stop the test after a specific number of failures occur by using the failure count setting. You can configure a test to run multiple times using the iteration setting.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**diagnostic ondemand {iteration** *iteration_count* } | {**action-on-error {continue | stop**}[*error_count*]} **Example:** `Router#` **diagnostic ondemand iteration 3**	Configures on-demand diagnostic tests to run, how many times to run (iterations), and what action to take when errors are found.
Step 3	**diagnostic start** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} • **diagnostic start** {**subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive | per-port** [**port** {num | *port#-range* | **all**}]} **Example:** `Router# diagnostic start bay 1/0 test 5`	Starts the on-demand diagnostic test on the specified bay, slot, or subslot.
Step 4	**diagnostic stop** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **Example:** `Router# diagnostic stop bay 1/0`	Stops the diagnostic test running on the specified bay, slot, or subslot.

Scheduling Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis. You can schedule tests to run only once or to repeat at an interval. Use the **no** form of this command to remove the scheduling.

To schedule online diagnostics, perform this task:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**diagnostic schedule** {**bay** *slot/bay* | **slot** *slot-no* } **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} {**daily** *hh:mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm* } **Example:** **diagnostic schedule** {**subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port** {**daily** *hh***:***mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm* | **port** {{*num* | *port#range* | **all**}{**daily** *hh***:***mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm*}}}} **Example:** `Router(config)#` **diagnostic schedule bay 1/0 test 1 on september 2 2009 12:00** **Example:** `Router(config)#` **diagnostic schedule slot 1 test complete daily 08:00**	This example shows how to schedule the diagnostic testing on a specific date and time for a specific bay: This example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific slot: Schedules on-demand diagnostic tests for a specific date and time, how many times to run (iterations), and what action to take when errors are found.

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing while the system is connected to a live network. You can configure the execution interval for each health monitoring test, whether or not to generate a system message upon test failure, or to enable or disable an individual test. Use the **no** form of this command to disable testing.

Note Before enabling the diagnostic monitor test, you first need to set the interval to run the diagnostic test. An error message is displayed if the interval is not configured before enabling the monitoring.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**diagnostic monitor interval** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all**} {*hh:mm:ss*} {*milliseconds*} {*number-of-days* **Example:** `Router(config)#` **diagnostic monitor interval bay 1/0 test 2 06:00:00 100 10**	Configures the health-monitoring interval of the specified tests. The **no** form of this command will change the interval to the default interval, or zero.
Step 4	**diagnostic monitor** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all**} **Example:** `The following example shows a sample output of an error message displayed when monitoring is enabled before configuring the test interval:` **Example:** `Router(config)#` **diagnostic monitor bay 1/0 test 2** `Aug 12 18:04:56.280: %DIAG-3-MONITOR_INTERVAL_ZERO: Bay 1/0: Monitoring interval is 0. Cannot enable monitoring for Test #2`	Enables or disables health-monitoring diagnostic tests.
Step 5	**diagnostic monitor syslog** **Example:** `Router(config)#` **diagnostic monitor syslog**	Enables the generation of a system logging messages when a health-monitoring test fails.
Step 6	**diagnostic monitor threshold** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot* } **test** {*test-id* | *test-id-range* | **all**} {**failure count** *no-of-allowed-failures* } **Example:** `Router(config)#` **diagnostic monitor threshold bay 1/0 test 2 failure count 10**	Configures the failure threshold value for the bay, slot, or subslot.

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured and check the results of the tests using the **show** commands.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show diagnostic content all** | bay *slot/bay* | slot *slot-no* | subslot *slot/subslot* **Example:** `Router#` **show diagnostic content bay 1/0**	Displays the online diagnostics tests and test attributes that are configured.
Step 3	**show diagnostic result** [[**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*] {**detail** | **test** {*test-id* | *test-id-range* | **all**}} | **all** **Example:** `Router#` **show diagnostic result all**	Displays the diagnostic test results (pass, fail, or untested) for a bay, slot, or subslot.
Step 4	**show diagnostic schedule all** | **bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*] **Example:** `Router#` **show diagnostic schedule slot 1**	Displays the current scheduled diagnostic tasks.
Step 5	**show diagnostic events** [**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot* | **event-type** {*error* | *info* | *warning*}] **Example:** `Router#` **show diagnostic events subslot 5/0**	Displays the diagnostic event log details for the specified bay, slot, or subslot.

Supported GOLD Tests on Cisco UBR10012 Router

This section discusses the GOLD test cases that have been implemented on Cisco UBR10012 Router in the Cisco IOS Release 12.2(33)SCC. This section contains the following topics:

Low Latency Queue (LLQ) Drop Test

To support the low latency requirements of voice calls the UBR10012 Router uses per interface absolute priority queues. Verifying the drops in the queue is a cumbersome manual process. Because of this, the periodic LLQ Drop test has been implemented to monitor all low latency queues on the box for drops. The test is a non-proxy test case that runs on the RP.

For the specified slot/subslot or slot/bay pair, the test will walk all associated forwarding interfaces legacy, modular, integrated, and wideband and look for drops on the interface low latency queue (if one exists). If drops are found, the test case reports a failure to the GOLD infrastructure and log a system log message with pertinent information.

Note The LLQ Drop test runs on demand with a default period of one (1) hour. It can be configured to run as often as every one minute.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 206: Hardware Support Matrix for LLQ Drop Test

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	Test520LLQDrops	For 5x20 line cards, the test returns per port results with a port corresponding to a downstream interface.
20x20 line card	Test2020LLQDrops	For 20x20 line cards, the test returns per port results with a port corresponding to a controller.
Modena SPA	TestModenaLLQDrops	On Modena SPA, the test returns global results.

Guardian Index Leak Test

For remote downstreams using SPAs, the Guardian maintains stat indices for remote service flows, PHS indices for voice flows on NB modems and BPI indices for encrypted modems. The index associations are maintained on the host mac-domain. There could be cases where the service flow has been destroyed or the cable modem has been kicked offline and the corresponding indices have not been de-allocated on the guardian. Any index leaks arising out of corner cases or race conditions would cause the index table to run out of indices which would then prevent any new modems to come online or new service flows to be created.

Periodic GOLD test (TestBlazeIndexLeak) has been introduced for 5x20 line cards to catch these index leaks early. TestBlazeIndexLeak test is a proxy test which runs on the linecard per slot or subslot. The number of Blaze indices are compared on each mac-domain host with the indices allocated by the guardian. If inconsistencies are found, error message is reported on the line card, with the mac-domain host inconsistencies. The error message displays the allocating guardian, the host line card on which the test fails and the margin observed.

Note The TestBlazeIndexLeak test runs on demand with a default period of eight (8) hours.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 207: Hardware Support Matrix for Guardian Index Leak Test

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	TestBlazeIndexLeak	For 5x20 line cards, the test returns per port results with a port corresponding to a downstream interface.

Memory Leak Test

As part of health monitoring tests, GOLD test case for detecting memory leaks in IOS have been added. The programmed approach covers potential leaks in IO Buffers and Processor Heap Memory. Most of the approaches to detect memory leak, require human analysis or tool based post-processing of outputs from various show commands. The Memory Leak Test adds a programmatic implementation inside IOS code itself to detect and signal any 'sizeable levels of IOS memory leaks' occurring over-time. The TestMemLeaks test case is automatically kick-started by GOLD on both PRE and CLC. One hour after card bootup, the test starts sampling free-memory data every 2 minutes in the background and then after every two hours it generates Leak test results for GOLD.

Test Result Behavior: The GOLD TestMemLeak failures are persistent failures, i.e. if the test fails due to a leak detected during a two hour window, the test fails from here on till card reboot, even if no new leaks were detected during ongoing two-hour sampling window.

Memory: The TestMemLeaks test adds some fixed-size static data-structures that take less than 10KB of fixed memory. To run per-RU-IO-buffer leak test, dynamic List is also allocated to get per-RU-stats, and these list elements are all freed before the test is over.

The Memory Resource Monitoring test case added as TestMemLeaks currently covers the following two approaches:

- Free Memory Trending, on page 1820
- I/O Memory Buffer Hold Accounting, on page 1821

Free Memory Trending

Aggregate level memory leaks can be detected using Free Memory Trending. Free memory trending requires system to get baseline usage numbers after one hour of system boot-up, and collect free memory samples every few minutes. Apply the free memory trending approach after you have enough samples. Periodically keep a watch on trend of free, lowest and largest block levels, by performing:

- Leak Trending check: Size of the Lowest Free Memory, Current Free Memory. Compare these samples to previous values and if all these parameters indicate a gradually leaking memory, and signal it as a test failure. If the following conditions are significantly found to be true, the logic alarms leaking memory.
    - FreeBytes of next sample are lower than FreeBytes of previous sample, AND

- Lowest free in this sample is within 10KB bytes of freeBytes; AND
- If lowest free in this sample is lesser than lowest block of previous sample
- If such conditions are found to be true for more than 25% of periodically collected samples, LeakTrend is assumed.

- Lower Threshold Check: Compare the free memory threshold to total memory on the card.

If the above two checks fail, a red flag is raised as an error message that memory on the box has been gradually leaking.

- If Largest Free is less than 1 MB (min. buffer size level for safe allocation) i.e. even if Largest free memory is above risk thresholds but if 'Lowest Sized buffer' reaches dangerous levels (like 1MB), then the logic signals memory leak error.

I/O Memory Buffer Hold Accounting

This section discusses, how I/O memory buffer leak scan algorithm works. To detect I/O memory leaks, besides the free-memory trending approach, the buffer life span analysis approach is also considered, where old buffers stored for more than a specified threshold of time are considered leaking. The command **show buffers leak resource** user displays a detailed summary of buffers that are older than a minute in the system, on a per Resource-User basis.

Note The TestMemLeaks test runs on demand with a default period of two (2) hours.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 208: Hardware Support Matrix for Memory Leak Detection

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	TestMemLeaks	Poll, collect, and compare samples of Processor Memory Leak and I/O Memory Buffer leak.
20x20 line card	TestMemLeaks	Poll, collect, and compare samples of Processor Memory Leak and I/O Memory Buffer leak.

How to Manage Diagnostic Tests

This section describes how to manage the diagnostic tests. The following GOLD commands are used to to manage the ondemand and periodic diagnostic tests:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**diagnostic ondemand** **Example:** `Router# diagnostic ondemand iteration 50`	Configures the ondemand diagnostic parameters such as iteration-count and action-on-error. These parameters signify the number of times the test is run and the execution action when a failure is detected. These parameters are used when the command **diagnostic start** is executed. In the given example, the iteration count to the same ondemand diagnostic test again is configured as 50. **Note** By default, iteration-count is 1, action-on-error is continue, and error count is 0.
Step 2	**show diagnostic ondemand settings** **Example:** `Router# show diagnostic ondemand settings`	Displays the ondemand diagnostic settings configured using the command **diagnostic ondemand**.
Step 3	**diagnostic start** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} **Example:** `Router# diagnostic start bay 1/0 test 1 all`	Starts an ondemand diagnostic test. • **bay** *slot/bay*—Indicates the card slot and bay number where the diagnostic test is executed. The bay keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number. • **slot** *slot-no*—Indicates the slot number of the full-height line card where the diagnostic test is executed. The slot keyword is used to refer a full-height line card on the router. The valid range for slot is from 1 to 8. • **subslot** *slot/sub-slot*—Indicates the slot and subslot number of half-height line card where the diagnostic test is executed. The subslot keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number. • **test—** Specifies a test to run. • *test-id*—Identification number for the test to run. • *test-id-range*—Range of identification numbers for tests to run. • **minimal—**Runs minimal bootup diagnostic tests. • **complete—**Runs complete bootup diagnostic tests. • **non-disruptive—**Runs the non disruptive health-monitoring tests. • **all—**Runs all diagnostic tests.
Step 4	**show diagnostic content** **Example:** `Router# show diagnostic content`	Displays the registered tests, attributes, and the configured interval at which the test runs. **Note** To view the registered test details for a specific SPA, full-height line card, or half-height line-card, use the keywords bay, slot, or subslot.

	Command or Action	Purpose
Step 5	**show diagnostic result** **Example:** `Router# show diagnostic result`	Displays the diagnostic test results for a SPA, full-height line card, or half-height line card.
Step 6	**show diagnostic events** **Example:** `Router# show diagnostic events`	Displays the diagnostic event log details for all the SPAs, full-height line card, and half-height line cards installed on the Cisco UBR10012 Router.
Step 7	**diagnostic stop** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} **Example:** `Router# diagnostic stop bay 1/0 all`	Stops the ondemand diagnostic test.
Step 8	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 9	**diagnostic bootup level** {**minimal** | **complete**} **Example:** `Router(config)# diagnostic bootup level complete`	Configures the bootup diagnostic level. • **minimal—**Specifies minimal diagnostics. • **complete—**Specifies complete diagnostics.
Step 10	**show diagnostic bootup level** **Example:** `Router# show diagnostic bootup`	Displays the configured bootup diagnostic level.
Step 11	**diagnostic event-log size** *size* **Example:** `Router(config)# diagnostic event log size 10000`	Modifies the diagnostic event log size dynamically. • *size***—**Diagnostic event-log sizes. The valid values range from 1 to 10000 entries.
Step 12	**diagnostic monitor interval** {**bay** *slot/bay* | **slot** *slot-no*} | **subslot** *slot/subslot*} **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds days* **Example:** `Router(config)# diagnostic monitor interval bay 1/0 test 2 06:00:00 100 20`	Configures the health monitoring diagnostic test interval to rerun the tests. • *hh:mm:ss***—**Hours, minutes, and seconds interval configured to run the test again. • *milliseconds***—**Number of milliseconds between tests. • *days***—**Number of days between tests. The valid range is from 0 to 20.

	Command or Action	Purpose
Step 13	**diagnostic schedule module** {module-number | slot/subslot} **test** {*test-id* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port**} **Example:** `Router(config)# diagnostic schedule slot 1 test complete daily 08:00`	Schedules the online diagnostic test to run at a designated time, or on daily, weekly or monthly basis. • *module-number*—Specifies the module number. • *per-port*—Selects the per-port test suite.
Step 14	**show diagnostic schedule** **Example:** `Router# show diagnostic schedule`	Displays the current scheduled diagnostic tests.

Configuration Examples for GOLD Feature

The following example shows a sample output of the test configuration, test attributes, and the supported coverage test levels for each test and for each bay/slot/subslot:

```
Slot 1: 2jacket-1
  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
                                                                      Test Interval
  ID   Test Name                                    Attributes      day hh:mm:ss.
  ==== ========================================== ============    =============
    1) TestJacketSample -------------------------> ***N****I       not configured  n/a
        Bay 1/0: 2jacket-1
          Diagnostics test suite attributes:
            M/C/* - Minimal bootup level test / Complete bootup level test / NA
              B/* - Basic ondemand test / NA
            P/V/* - Per port test / Per device test / NA
            D/N/* - Disruptive test / Non-disruptive test / NA
              S/* - Only applicable to standby unit / NA
              X/* - Not a health monitoring test / NA
              F/* - Fixed monitoring interval test / NA
              E/* - Always enabled monitoring test / NA
              A/I - Monitoring is active / Monitoring is inactive
                                                                                Test
 Interval
            ID   Test Name                                    Attributes      day
hh:mm:ss.
           ==== ========================================== ============    ====
=========
             1) TestModenaSample -------------------------> ***N****I       not configured
  n/a
            2) TestModenaLLQDrops ----------------------> ***N****A       000 01:00:00.00
 1
```

Additional References

For additional information related to health monitoring, see the following references:

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
System Event Archive (SEA)	SEA feature for the Cisco UBR10012 Router

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for GOLD for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 209: Feature Information for GOLD for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Generic Online Diagnostic (GOLD) subsystem support for the Cisco CMTS Routers	12.2(33)SCC	GOLD is a health monitoring feature implemented to run diagnostic tests and poll for system components, which do not generated errors. This feature was introduced for the MC5x20, MC20x20 cable line cards, Modena SPA, Jacket cards, PRE2, and PRE4 route processors. The following commands are new or modified: • **diagnostic start** • **diagnostic stop** • **diagnostic ondemand** • **show diagnostic bootup** • **show diagnostic content** • **show diagnostic description** • **show diagnostic events** • **show diagnostic ondemand** • **show diagnostic result** • **show diagnostic schedule** • **diagnostic bootup** • **diagnostic event-log** • **diagnostic monitor** • **diagnostic schedule**

CHAPTER 73

Managing Cable Modems on the Hybrid Fiber-Coaxial Network

After you have completed upstream and downstream configuration you have additional options to manage how your CMs operate in the hybrid fiber-coaxial (HFC) network. You can set the following CM functions:

Section	Purpose
t_Activating_CM_Authentication_1041780.xml#con_1041780	Configures the Cisco uBR10000 series CMTS to require all CMs to return a known text string to register with the CMTS and gain access to the network.
t_Activating_CM_Authentication_1039189.xml#con_1039189	Configures the Cisco uBR10000 series CMTS to require all CMs to return a known text string to register with the CMTS and gain access to the network.
t_Activating_CM_Insertion_Interval_1039220.xml#con_1039220	Limits the amount of time that a CM requests a channel for the first time from the Cisco uBR10012 router. (A CM's initial channel request is known as insertion.)
t_Activating_CM_Upstream_Address_Verification_1039314.xml#con_1039314	Ensures that only CMs that have received DHCP leases through the Cisco uBR10000 series CMTS can access the HFC network.
r_Clearing_CM_Counters_1039366.xml#con_1039366	Clears the counters for the CMs in the station maintenance list.
r_Clearing_CM_Reset_1039411.xml#con_1039411	Removes one or more CMs from the station maintenance list and resets the cable modem (or all CMs) on the network.
t_Configuring_CM_Registration_Timeout_1039439.xml#con_1039439	Specifies the registration timeout interval for CMs connected to the Cisco uBR10012 router.

Section	Purpose
t_Configuring_Dynamic_Contention_Algorithms_1039463.xml#con_1039463	Configures the algorithms that control the capacity of the contention subchannel and how efficiently a given contention subchannel capacity is used.
t_Configuring_the_Dynamic_Map_Advance_Algorithm_1039513.xml#con_1039513	Enhances the upstream throughput from a CM connected to the Cisco uBR10000 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAC allocation and management messages (MAPs), based on several input parameters for the corresponding upstream channel.
t_Configuring_Maximum_Hosts_Attached_to_a_CM_1039542.xml#con_1039542	Specifies the maximum number of hosts that can be attached to a subscriber's CM.
t_Configuring_Per-Modem_Filters_1039559.xml#task_1039559	Provides instructions to configure the Cisco uBR10012 router to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address.
t_Configuring_Sync_Message_Interval_1039622.xml#con_1039622	Specifies the sync message interval between successive sync message transmissions from the Cisco uBR10000 series CMTS.

Note Cisco recommends using default values for most commands. The default values for the commands used in these configuration steps are, in most cases, adequate to configure the Cisco uBR10012 router.

Note For information about setting rate limiting on CMs, refer to these sections in Chapter 3:

- t_Setting_Downstream_Traffic_Shaping_1061062.xml#con_1061062
- t_Setting_Upstream_Traffic_Shaping_1055032.xml#task_1055032

Content

Activating CM Authentication

The Cisco uBR10012 router can be configured to require all CMs to return a known text string to register with the CMTS and gain access to the network. The text string can be from 1 to 80 characters in length. To activate CM authentication, use the following command from cable interface configuration mode.

To configure authentication and data privacy parameters, use the cable shared-secret command in cable interface configuration mode. To disable authentication during the CM registration phase, use the no form of this command.

cable shared-secret [**0** | **7**] *authentication-key*

no cable shared-secret

0	(Optional) Specifies that an unencrypted message will follow.
7	(Optional) Specifies that an encrypted message will follow.
authentication-key	Text string is a shared secret string. When you enable the service password-encryption option, the password is stored in encrypted form. The text string is a 64-character authentication key.

The following example shows how to activate CM authentication using 3344912349988...sf as the shared secret key and indicating that an encrypted message follows:

```
Router(config-if)# cable shared-secret 7 3344912349988cisco@xapowenaspasdpuy230jhm...sf
```

Verify CM Authentication

To verify whether CM authentication is activated or deactivated, enter the command **more system:running-config** and look for the cable interface configuration information. If CM authentication is deactivated, it appears in this output as no cable secret-shared.

Activating CM Insertion Interval

When a CM is ready to transmit data, it requests a channel from the Cisco uBR10012 router. You can limit the amount of time that a CM requests a channel for the first time from the Cisco uBR10012 router. A CM's initial channel request is known as insertion. The valid range is 100 to 2000 milliseconds.

To activate the CM insertion interval, use the following command in cable interface configuration mode.

Command	Purpose
cable insertion-interval milliseconds	Sets the insertion interval in milliseconds.

Validating CM Insertion Interval

To verify that a CM insertion interval has been set, enter the command **more system:running-config** command, and look for the cable interface configuration information, as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Troubleshooting CM Insertion Interval

If you are having trouble, make sure that you entered the correct slot and port numbers when you typed the command.

Activating CM Authentication

The Cisco uBR10000 series CMTS can be configured to require all CMs to return a known text string to register with the CMTS and gain access to the network. The text string can be from 1 to 80 characters in length. The default setting is "on" (CM authentication is activated).

To activate CM authentication, use the following command in cable interface configuration mode:

Command	Purpose
cable shared-secret [0|7] authorization-key **no cable shared-secret**	Enables CM authentication: • **0** specifies an unencrypted authentication key. • **7** specifies an encrypted authentication key. Disables CM authentication.

Tip Be sure that you enter the correct slot and port number in cable interface configuration mode. Verify that the CM is using baseline privacy interface (BPI) and that it is assigned to a quality of service (QoS) with privacy active. Verify that the cable interface configuration file contains a matching key.

Verifying CM Authentication

To verify if CM authentication has been activated or deactivated, enter the command more system:running-config and look for the cable interface configuration information. If CM authentication has been activated, it does not appear in this output. If CM authentication has been deactivated, it appears in this output as " no cable secret-shared ," as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
  no cable secret-shared
  cable insertion-interval 150000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Troubleshooting CM Authentication

If you are having trouble, make sure that you entered the correct slot and port numbers when you entered cable interface configuration mode.

For additional troubleshooting information, refer to Chapter 6, "Troubleshooting the System."

Activating CM Upstream Address Verification

CM upstream address verification ensures that only CMs that have received Dynamic Host Configuration Protocol (DHCP) leases through the Cisco uBR10012 router can access the HFC network. The Cisco uBR10012 router discards all packets received from or for hosts that have not received Dynamic Host Configuration Protocol (DHCP)-assigned addresses. The default setting is "off" (CM upstream address verification is deactivated).

To activate or deactivate CM upstream verification, use the following command in the cable interface configuration mode:

Command	Purpose
cable source-verify [dhcp]	Activates CM upstream verification. The **dhcp** option specifies that queries be sent to verify unknown IP addresses in upstream data packets.
no cable source-verify	Returns to the default upstream verification state.

Verifying CM Upstream Address Verification

To verify that CM upstream verification has been activated or deactivated, enter the command **more system:running-config** and look for the **no cable source-verify** notation in the cable interface configuration information. If CM upstream verification has been deactivated, it does not appear in this output. If CM upstream verification has been activated, it appears in this output as **cable source-verify**, as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
  cable source-verify
  cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Tip Be sure that you enter the correct slot and port number when you enter the cable interface configuration mode.

Note If the Cisco uBR10012 router is reloaded or the Address Resolution Protocol (ARP) table is cleared, all hosts on the network are forced to release and renew their IP addresses. Some systems might require restarting if the IP protocol stack is unable to renew using a broadcast IP address.

Clearing CM Counters

To clear the counters for the CMs in the station maintenance list, use one of the following commands in cable interface configuration mode.

Command	Purpose
clear cable modem *mac-addr* **counters**	Clears the counters in the station maintenance list for the CM with a specific MAC address.
clear cable modem *ip-addr* **counters**	Clears the counters in the station maintenance list for the CM with a specific IP address.
clear cable modem all counters	Clears the counters in the station maintenance list for all CMs.

Verifying Clear CM Counters

To determine if the counters in the station maintenance list are cleared, enter one of the following commands. The station maintenance list counter is 0.

Command	Purpose
`show cable modem` *ip-address*	Displays the status of a CM identified by its IP address.
`show cable modem` *mac-address*	Displays the status of a CM identified by its MAC address.
`show cable modem` *interface-address*	Displays the status of all CMs on a particular upstream.

Clearing CM Reset

To remove one or more CMs from the station maintenance list and reset the cable modem (or all CMs) on the network, use one of the following commands in cable interface configuration mode.

Command	Purpose
`clear cable modem` *mac-addr* `reset`	Removes the CM with a specific MAC address from the station maintenance list and resets it.
`clear cable modem` *ip-addr* `reset`	Removes the CM with a specific IP address from the station maintenance list and resets it.
`clear cable modem all reset`	Removes all CMs from the station maintenance list and resets them.

Verifying Clear CM Reset

To determine if the **clear cable modem reset** command has removed a CM from the station maintenance list and forced it to start a reset sequence, enter the **show cable modem** command.

Tip Be sure that you entered the correct CM IP address or MAC address when you typed the **clear cable modem reset** command. It might take up to 30 seconds for the CM to start the reset sequence.

Note The **clear cable modem reset** command is useful if a Simple Network Management Protocol (SNMP) manager is not available, or if the CM is unable to obtain an IP address or respond to SNMP messages.

Configuring CM Registration Timeout

By default, registered CMs that have no upstream activity for three minutes are timed out and disconnected from the Cisco uBR10012 router. This timeout interval can be decreased to 2 minutes or increased up to 60 minutes.

To specify the registration timeout interval for CMs connected to the Cisco uBR10012 router, use the following command in cable interface configuration mode.

Command	Purpose
`cable registration-timeout` *n*	Specifies the maximum number of minutes allowed to elapse with no upstream activity before terminating the connection. Valid range is from 2 to 60 minutes. Default = 3 minutes.

Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff)

The Cisco uBR10000 series software includes the following algorithms that control the capacity of the contention subchannel and control the efficient use of a given contention subchannel capacity:

- Algorithm that dynamically controls the rate of upstream contention slots—initial ranging and bandwidth requests.
- Algorithm that varies the backoff parameters that CMs use. Backoff variation falls within each of the initial ranging and bandwidth request upstream contention subchannels.

In high contention mode, the Cisco uBR10000 series MAC scheduler uses collision statistics and sustains a high frequency of initial ranging slots until it detects a steady ranging state. The CMTS dynamically varies the frequency of initial ranging slots using the data grant utilization on the upstream channels. The CMTS trades upstream bandwidth between data grants and initial ranging slots. The CMTS autodetects a high collision state and switches to low insertion interval mode after a steady state is achieved where few collisions occur.

The CMTS is careful when monitoring the ranging channel health to revert to a steady state. In steady state mode, data grants—grant utilization—receive preference over initial ranging slots.

Although the binary exponential backoff algorithm operates in a distributed fashion at different CMs, the CMTS provides centralized control for the backoff algorithm. To achieve this, it remotely monitors traffic load—the backlog developing on the contention channel—and then varies the backoff start and end specified in the MAPs for that upstream channel. This ensures that colliding CMs are properly randomized in time.

The following cable interface commands are available to configure the dynamic contention algorithms:

```
[no] cable insertion-interval [automatic [Imin [Imax]]] | [msecs]
[no] cable upstream port num range-backoff [automatic] | [start end]
[no] cable upstream port num data-backoff [automatic] | [start end]
```

cable insertion-interval Command Examples

To deviate from system defaults when modifying the dynamic contention algorithm, use one of the **cable insertion-interval** command in cable interface configuration mode. For more information on the command, see cable insertion-interval command.

Tip System defaults are to have dynamic ranging interval enabled, dynamic ranging backoff enabled, and fixed data backoffs for each upstream of a cable interface.

The default automatic insertion interval setting enables the Cisco automatic initial ranging period algorithm, where lower and upper default values of 60 msecs and 480 msecs are used. The default **automatic range-backoff** setting enables the dynamic backoff algorithm.

Configuring the Dynamic Map Advance Algorithm

A Cisco CMTS administrator can enhance the upstream throughput from a CM connected to the Cisco uBR10000 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.

Caution Only a trained Cisco CMTS administrator should adjust these values.

To configure the dynamic map advance algorithm, use the following command in cable interface configuration mode.

Command	Purpose
`cable map-advance dynamic [n]|static`	Specifies a value to enhance the upstream throughput from a CM connected to the Cisco uBR10012 router. The *n* argument provides the safety factor for the dynamic map advance algorithm. This argument is specified in usecs and controls the amount of extra lookahead time in MAPs to account for inaccuracies of the measurement system and software latencies. The default value is 1000 usecs. You can vary this value from 500 to 1500 usecs. This argument is a delta value added to the dynamic **map-advance** setting that the algorithm computes. Using larger safety factors increases the run-time lookahead in MAPs, but reduces the upstream performance. Use the static keyword for the cable map-advance command. The Cisco uBR10012 router uses a fixed lookahead time in MAPs, regardless of the real propagation delay of the farthest CM on the network. This fixed lookahead time is computed based on the worst-case parameters, such as farthest DOCSIS propagation delay for the CMs.

Caution If you are adjusting the dynamic map-advance algorithm, do not reduce the safety factor below the default value of 1000 usecs in a production network, until you are confident that the reduced safety factor suffices for your deployment. The default value is chosen to be a safe operating point for the algorithm.

Configuring Maximum Hosts Attached to a CM

To specify the maximum number of hosts that can be attached to a subscriber's CM, use the following command in cable interface configuration mode.

Command	Purpose
`cable max-hosts n` `no cable max-hosts`	Specifies the maximum number of hosts that can be attached to a CM on this interface. Valid range is from 0 to 255 hosts. Default = 0. Resets the allowable number of hosts attached to a CM to the default value of 0 hosts.

Configuring Per-Modem Filters

You can configure the Cisco uBR10012 router to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. Definition of filters follows standard Cisco IOS configuration practices for access lists and groups.

Note Configuring per modem or host filters is supported in Cisco IOS Release 12.0(5)T1 or higher, as well as in Cisco IOS Release 12.0(6)SC or higher.

To configure per modem filters, use the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cable** {**modem** | **host** | **device**} {*macaddr ipaddr* | } **access group** *acl*	Configure 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 the packets are received from. Use modem if the device is a CM. Use host if the device is a CPE device attached to a CM. Define the filter to be applied to the device and a given address. The macaddr specifies the CM's or CPE device's unique MAC address. Use the ipaddr option to specify the CM or CPE device's current IP address. Use the acl option to assign the CM or CPE device to an access list. This defines the per-CM or per-host filter requirements implemented at the CMTS, rather than at the CM. Access list numbers are 1 to 99 for fast IP access lists, 100 to 199 for show extended IP access lists. **Note** Access list numbers of 700 to 799 do not apply.

What to Do Next

Caution The system applies filters after the CM registers with the CMTS. Filter definitions are not saved across system reboots and must be applied each time a CM registers.

The software supports traps to alert CMTS administrators on CMs going offline or back online. A typical registration and login procedure is shown below:

1. The CM registers with the Cisco uBR10000 series.
2. The Cisco uBR10000 series sends traps to management systems in use for the network.
3. The management system sets per modem filters using SNMP or rsh.
4. The user logs in at the server.
5. The login server obtains required modem and CPE information from the Cisco uBR10000 series.
6. The login server sets per-CPE filter in the Cisco uBR10000 series. The per-CPE filter overrides the per modem filter settings.
7. If the CM goes offline for a brief period of time, filters defined using the Cisco uBR10000 series remain active. If a CM stays offline for more than 24 hours, filter settings are reset.
8. If the user logs out or the login server detects that the user is not online, the login server sets default filters for the CM or the CPE device.

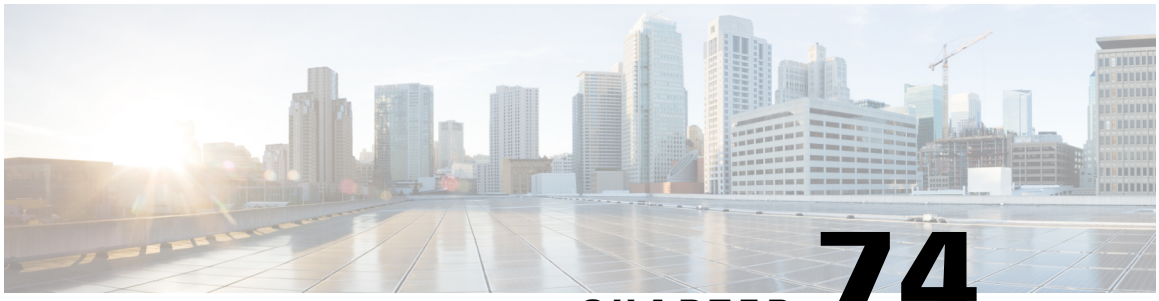
Configuring Sync Message Interval

To specify the sync message interval between successive sync message transmissions from the Cisco uBR10012 router, use the following command in cable interface configuration mode.

Command	Purpose
`cable sync-interval msec` **`no cable sync-interval`**	Specifies the interval in milliseconds between successive sync message transmissions from the Cisco uBR10000 series CMTS. Valid values are from 1 to 200 msec. Default = 10 msec. Returns the sync message interval to its default value of 10 msec.

Verifying Sync Message Interval

To determine if a sync message interval is configured, enter the **show running-config** command and look for the cable interface configuration information. If the sync message interval is deactivated or reset to its default value, the no sync interval command line appears in the output.



CHAPTER 74

Maximum CPE and Host Parameters for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 23, 2013

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to use different methods to control subscriber access that are allowed by the Data-over-Cable Service Interface Specifications (DOCSIS) for use on cable networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Maximum CPE and Host Parameters for the Cisco CMTS Routers

The Maximum CPE and Host Parameters for the Cisco CMTS Routers feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table shows the hardware compatibility prerequisites for this feature.

Table 210: Maximum CPE and Host Parameters for the Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE-2 Cisco IOS Release 12.2(33)SCB and later • PRE-4 Cisco IOS Release 12.2(33)SCH and later • PRE-5	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V1
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Information About the MAX CPE and Host Parameters

The DOCSIS specification includes a number of provisions to allow service providers to control the number of subscribers who can access the network through any particular cable modem.

The following are the parameters that controls the number of CPE that can access the network:

Note In addition, the DOCSIS configuration file contains a Network Access parameter that specifies whether the CPE devices behind the cable modem can access the cable network. If the Network Access parameter is set to Disabled, no CPE devices behind a cable modem are able to access the network.

Tip Also, the Cisco CMTS lists offline cable modems in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hour period expires, the CMTS continues to use the existing CPE counts.

All of these methods are similar in purpose, but they are configured differently and have a different impact on cable modems and their CPE devices.

The cable modem enforces the MAX CPE and MAC CPE IP values, and the CMTS enforces the MAX Host value. Because CPE devices can come online and offline at any time, it is important to understand how these different parameters interact, and how the cable modem and CMTS enforce them.

Note The MAX CPE parameter provides Layer 2 control of CPE devices. The MAX CPE IP parameter provides Layer 3 control of CPE devices. The two methods are complimentary but not otherwise related.

MAX CPE

The MAX CPE is a required parameter and used to control the number of CPE devices that can access the network during the current session. In DOCSIS 1.0 cable networks, the MAX CPE parameter is the primary means of controlling the number of CPE devices that can connect to the cable network using any particular cable modem. This parameter is configured in the DOCSIS configuration file (TLV 18). If this parameter is not specified in the DOCSIS configuration file, it defaults to a value of 1.

Note In DOCSIS 1.1 cable networks, the CMTS ignores the MAX CPE parameter that is specified in the DOCSIS configuration file, and uses the MAX CPE IP, on page 1844 parameter instead.

Each time a new CPE device attempts to connect to the cable network, the cable modem logs the hardware (MAC) address. If the cable modem has not reached the MAX CPE number of MAC addresses, the new CPE device is allowed to access the network. If the cable modem has reached the MAX CPE limit, it drops the traffic from any additional CPE devices.

By default, the cable modem learns new MAC addresses on a first-come, first-served basis. You can also preconfigure the allowable MAC addresses for CPE devices by entering those MAC addresses in the DOCSIS configuration file (TLV 14). These cable modem gives these preconfigured MAC addresses preference in connecting to the network.

The DOCSIS specification does not allow cable modems to age out MAC addresses, so a MAC address stays in the log table of the cable modem until the cable modem is reset. You should therefore think of this parameter as specifying the maximum number of CPE devices that can connect during any particular session, instead of the maximum number of CPE devices that can simultaneously connect to the cable network.

For example, if you set MAX CPE to 2, a customer could use their cable modem to connect a maximum of two CPE devices (two MAC addresses) to the cable network. A customer could choose to connect two PCs simultaneously to their cable modem and use both to access the network.

However, if the customer then disconnected these PCs and connected two new PCs, the cable modem would not allow the new PCs to come online, because they would be the third and fourth MAC addresses that are connected to the cable modem. The customer would have to reset the cable modem before being able to use the new PCs.

Note The MAX CPE value, if present, must be a positive integer in DOCSIS 1.0 configuration files. This parameter can be zero in DOCSIS 1.1 configuration files, but if so, the cable modem uses a MAX CPE value of 1. If the MAX CPE parameter is not present in either type of DOCSIS configuration file, it defaults to 1.

MAX CPE IP

The MAX CPE IP parameter is applicable only in DOCSIS 1.1 cable networks and is an optional parameter. This parameter specifies whether the cable modem should perform IP address filtering on the CPE devices. If so, this attribute also specifies the maximum number of simultaneous IP addresses that are permitted behind the modem at any one time.

The MAX CPE IP parameter is configured in the DOCSIS configuration file (TLV 35), or by using SNMP commands to set the docsDevCpeIpMax attribute (in DOCS-CABLE-DEVICE-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless you enable the use of the MAX CPE IP parameter by using the **cable submgmt default active** command.

Note In DOCSIS 1.1 networks, the CMTS ignores the MAX-CPE value (TLV 18) from the DOCSIS configuration file and uses the MAX CPE IP value instead.

If this feature is enabled, the cable modem learns the allowable IP addresses the first time that the CPE device sends an IP packet out into the network. The IP addresses are added to the docsDevFilterCpeTable table. This address table is cleared automatically when the cable modem is reset or powered off, or you can manually clear the IP address table by setting the docsSubMgtCpeControlReset attribute in the appropriate table entry for this cable modem.

In DOCSIS 1.1 networks, the MAX CPE IP parameter can be configured as follows:

- If MAX CPE IP is set to –1, the cable modem does not filter any IP packets on the basis of their IP addresses, and CPE IP addresses are not added to the modem's CPE address table
- If MAX CPE IP is set to 0, the cable modem does not filter any IP packets on the basis of the IP addresses. However, the source IP addresses are still entered into the modem's CPE address table.
- If MAX CPE IP is set to a positive integer, it specifies the maximum number of IP addresses that can be entered into the modem's CPE address table. The modem compares the source IP address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise, the packet is dropped.

Tip In Cisco IOS Release 12.2(8)BC1, a similar address filtering mechanism exists on the CMTS. See the description of the docsSubMgtCpeControlMaxCpeIp attribute in the DOCS-SUBMGT-MIB MIB for details.

The CMTS uses the MAX CPE IP value as part of its own filtering process, but the two filters operate independently on the cable modem and CMTS.

MAX CPE IPv6

The MAX CPE IPv6 parameter is an optional parameter and specifies the maximum number of simultaneous IPv6 addresses that are permitted for a cable modem at any time.

The MAX CPE IPv6 parameter is configured in the DOCSIS 3.0 configuration file (TLV 63), or by using the SNMP commands to set the docsSubmgt3BaseCpeMaxIpv6PrefixDef attribute (in DOCS-SUBMGT3-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless the use of the MAX CPE IPv6 parameter is enabled by using the **cable submgmt default active** command.

When the MAX CPE IPv6 feature is enabled, the cable modem learns the allowable IPv6 addresses the first time that the CPE device sends an IPv6 packet out into the network. The IPv6 addresses are added to the IPv6 address table. The address table is cleared automatically when the cable modem is reset or powered off.

In DOCSIS 3.0 networks, the MAX CPE IPv6 parameter can be configured as follows:

- If MAX CPE IPv6 is set to 0, the cable modem filters any IPv6 packets on the basis of the IPv6 addresses. All the source IPv6 addresses are not entered into the CPE address table of the cable modem.
- If MAX CPE IPv6 parameter is set to a positive integer, the parameter specifies the maximum number of IPv6 addresses that can be entered into the CPE address table of the cable modem. The modem compares the source IPv6 address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise the Cisco CMTS ignores the DHCPv6 packets from the CPE.

MAX Host

The MAX Host parameter is an optional parameter and is configured on the Cisco CMTS and specifies the maximum number of CPE devices (MAC addresses) that the CMTS will allow to have network access. You can control this parameter for individual cable modems, for all cable modems on a particular cable interface, or for all cable modems on the Cisco CMTS, depending on the CLI command being used:

- **cable modem max-hosts—**Configures MAX Host for a particular cable modem.
- **cable max-hosts—**Configures MAX Host for all cable modems on a particular cable interface.
- **cable modem max-cpe—**Configures MAX Host for all cable modems on the Cisco CMTS. You can use the **unlimited** keyword to specify that the Cisco CMTS should not enforce a MAX Host limit for cable modems.

When this is enabled, the Cisco CMTS learns a MAC address the first time that the CPE device accesses the cable network. After the Cisco CMTS has logged the maximum number of MAC addresses specified by a MAX Host parameter, it drops all traffic from CPE devices that have any other MAC address.

Tip In DOCSIS 1.1 cable networks, when both the MAX CPE IP and MAX Host parameters are configured, the Cisco CMTS uses the lesser value to determine the maximum number of CPE devices that are allowed behind each cable modem.

Note The entire MAX Host address table is cleared whenever the Cisco TS is reset. You can also clear an entry for a particular CPE device using the **clear cable host** command.

Specifying MAX Host and MAX CPE Values

Typically, you would set the MAX Host parameter to a number that is greater than the value for the MAX CPE of the cable modem or MAX CPE IP parameter. This would allow customers to switch between multiple computers, without requiring them to reboot their cable modem, and without requiring any action on the part of the service provider's network administrators.

For example, if you set MAX CPE or MAX CPE IP to a value of 2 for a cable modem, then you could set the MAX Host parameter to a value of 4. This would enable the cable modem to connect four different CPE devices to the cable network, but only two of them could be online simultaneously.

However, if you set the MAX Host parameter to a number smaller than the value of MAX CPE or MAX CPE IP in the DOCSIS configuration file, then the MAX CPE or MAX CPE IP value always takes precedence. For example, if the MAX CPE value is 2 and the MAX Host value is *1* , both the cable modem and CMTS allow up to two CPE devices to pass traffic for that cable modem.

Specifying an Unlimited Value for Max Host

The **cable modem max-cpe** command, which affects all cable modems on the CMTS, supports the **unlimited** keyword, which specifies that the CMTS should not enforce any limit on CPE devices. When you configure the CMTS with the unlimited **keyword**, this setting, you are allowing cable modems to support any number of CPE devices.

Do not use the **unlimited** option without also specifying the proper value for MAX CPE in the DOCSIS configuration file, so that each cable modem can control the maximum number of CPE devices it supports. In addition, to prevent users from requesting an unlimited number of IP address, be sure to configure the DHCP servers so that they control how many IP addresses are assigned to the CPE devices behind each cable modem.

Interoperation of the Maximum CPE Parameters

The different methods of CPE control can all be active simultaneously. They can interact with one another but do not conflict with one another. The table lists each method and compares their characteristics.

Table 211: Comparison of the Different Max CPE and Max Host Control Mechanisms

Method	Configuration Method	Function	Can Be Changed By...
Methods that are configured on the cable modem:			

Method	Configuration Method	Function	Can Be Changed By...
Network Access Control	DOCSIS Configuration File	Prevents all network access for CPE devices	Reset of cable modem
MAX CPE	DOCSIS Configuration File	Limits MAC addresses (Layer 2 control)	Reset of cable modem
MAX CPE IP	DOCSIS Configuration File SNMP Set Command	Limits IP addresses (Layer 3 control)	SNMP Set Command
Methods that are configured on the CMTS: [154]			
MAX CPE IP (the CMTS uses this value if MAX CPE IP is not specified in the DOCSIS configuration file)	DOCSIS Configuration File CLI Command SNMP Set Command	Limits IP addresses (Layer 3 control)	CLI Command SNMP Set Command
MAX Host Parameters			
MAX Host for one cable modem (**cable modem max-hosts**)	CLI Commands	Limits CPE devices for one particular cable modem	New CLI Command
MAX Host for a cable interface (**cable max-hosts**)		Limits CPE devices for all cable modems on a particular cable interface	
MAX Host for a CMTS (**cable modem max-cpe**)		Limits CPE devices for all cable modems on a Cisco CMTS	

154 In Cisco IOS Release 12.2(4)BC1 and later releases, the Cisco CMTS does not actively manage CPE devices unless this has been enabled using the cable submgmt default active command.

The table lists the MAX CPE parameters in order of priority. For example, the Network Access Control and MAX CPE parameters interact as follows:

- If the Network Access Control field for a cable modem is set to Disabled, none of that modem's CPE devices will be able to access the network, regardless of how the other parameters are set.
- If Network Access Control is Enabled and MAX CPE is set to 1 for a cable modem, then a maximum of one CPE device will be able to access the network, no matter how the remaining parameters are configured.

The table also lists the MAX Host parameters in order of more specific to less specific, where the more specific override the settings of the less specific. For example, if you use the **cable modem max-cpe** command to set the MAX Host value for all CMs to 2, you can still use the **cable modem max-hosts** command to give a particular CM a MAX Host value of 8.

In addition, the MAX CPE IP and MAX Host parameters interact as follows:

- When both the MAX CPE IP parameter and the MAX Host parameter for a specific cable modem are specified, the CMTS uses the value specified for MAX Host for that particular modem.
- When both the MAX CPE IP parameter and the MAX Host parameter for a cable interface are specified, the CMTS uses the larger value of the two.
- When both the MAX CPE IP parameter and the MAX Host parameter for the CMTS are specified, the CMTS uses the smaller value of the two.

Tip The Cisco CMTS keeps inactive cable modems listed in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hours expires, the CMTS continues to use the existing CPE counts.

Possible Conflicts Between Parameters

The recommended procedure for disconnecting one PC from a cable modem and reconnecting a new one is the following:

1. The user first releases the IP address assigned to the PC. The user can do this either by using a utility such as winipcfg, or by shutting down the PC.
2. The user disconnects the old PC and reconnects the new PC to the cable modem.
3. The user reboots the cable modem so as to clear out its MAX CPE values.
4. After the cable modem has come online, the user boots the new PC so that it can obtain the correct IP address and come online.

This procedure allows the MAX CPE value on the cable modem to stay synchronized with the MAX Host value on the CMTS. Problems can occur in the following situations:

- If the user does not release the IP address from the old PC before connecting a new one, the CMTS is not informed that the new PC is replacing the old one, and therefore counts both PCs when calculating the Host value. If the new value exceeds the MAX Host value, the CMTS does not allow the new PC to come online. The service provider has to issue the **clear cable host** command to remove the old PC from the MAX Host table, so as to allow the new PC to come online.
- If the user does not reboot the cable modem after disconnecting the old PC, the cable modem retains the old PC's MAC address and continues to count it when calculating the CPE value. If the new value exceeds the MAX CPE value, the cable modem does not allow the new PC to come online. The user has to reboot the cable modem before the new PC comes online.
- If the user booted their PC before turning on the cable modem or before connecting the Ethernet cable to the cable modem. In this case, the operating system typically assigns a static private IP address (such as 169.254.232.199, which is the default Windows IP address). When the cable modem then boots or is connected to the PC, it logs the PC's private IP address as one of the allowable IP addresses. So, if MAX CPE IP is set to 1, the PC will not be allowed access to the Internet. You must reboot the cable modem to clear its IP address tables, and allow the PC to acquire an IP address from the DHCP server. (To avoid this problem, set the docsDevCpeIpMax attribute for the cable modem to –1 in the DOCSIS configuration file. CableLabs has proposed –1 as the new default, but this change has not yet been given final approval or been implemented in current software releases.)

To reduce service-impacting problems when users replace PCs without following the above guidelines, service providers can configure the MAX Host parameter for a value greater than the MAX CPE value. This allows users to replace a limited number PCs without releasing the IP address and still be able to come online. (Users should continue to reboot the cable modem, however, because that is the only way to clear their internal CPE counter.)

For example, if you configure MAX CPE for a cable modem at 2, and MAX Host at 4, the user can connect any two PCs to the cable modem at any one time. The user can then replace both PCs with new PCs, reboot the cable modem, and have both PCs come online.

The CMTS CPE table for this cable modem lists all four PCs, and the user can switch between them at will, as long as the user reboots the cable modem after each switch. The user, however, is not allowed to bring a fifth PC online until one of the previous PCs has been cleared from the CMTS, using the **clear cable host** command.

Note The cable modem always enforces the MAX CPE parameter, regardless of the setting of the other parameters.

Summary of CPE Address Control

In DOCSIS 1.1 cable networks, CPE address control is done as part of the following process, which also includes Layer 2 and Layer 3 filtering:

1. MAC address filtering—Packets are filtered on the basis of the MAC address for the CPE device. The filter is controlled by the MAX CPE parameter, as set in the DOCSIS configuration file.
2. Logical Link Control (LLC) filtering—Packets are filtered on the basis of the protocol for the packets. The filter is controlled by the docsDevFilterLLCTable table on the cable modem.
3. CPE IP address filtering—Packets are filtered on the basis of the IP address for the CPE device, as controlled by the MAX CPE IP value, as well as the docsDevCpeIpMax attribute and the docsDevFilterCpeTable table on the CMTS.
4. Access list filtering—Packets are filtered on the basis of access lists. IP filtering is controlled by the docsDevFilterIpTable table, and SNMP access filters are controlled by the docsDevNmAccessTable table.
5. MAX Host control—The CMTS allows access for CPE devices on the basis of the MAX Host parameters.

Tip This document does not describe the LLC and access list filtering. For more information about these filters, see the DOCS-CABLE-DEVICE-MIB MIB for more information on the SNMP attributes and tables that are listed above.

Benefits

- CMTS flexibility allows multiple service operator provisioners, service providers, and other users to synchronize between the CMTS and the cable modem the maximum number of permitted CPE devices that can be connected behind a cable modem.
- Changes can be made by using CLI commands or by using SNMP commands.

How to Configure the MAX CPE and Host Parameters

To reset the maximum number of permitted CPE devices recognized by the CMTS, use one of the following configuration commands. All procedures are optional, depending on the requirements.

Note The CMTS assigns the MAX Host value to a cable modem at the time that the cable modem registers with the CMTS. Changing any of the MAX Host commands affects only cable modems that register after the change.

Configuring the Maximum Number of CPE Devices on the Cisco CMTS

To configure the maximum number of CPE devices per cable modem, use the following procedure:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modem max-cpe** [*number* | **unlimited**] **Example:** `Router(config)# cable modem max-cpe 8`	Sets the value of the MAX CPE parameter on the Cisco CMTS for all cable interfaces. The **show cable modem subscriber** displays the MAXIMUM value of cable modem max-cpe and the MAX CPE value in the DOCSIS configuration file of the cable modem. The number of the CPE that can be online is determined by the MAX CPE value in the DOCSIS configuration file of the cable modem. CBR lets MAX to be the number of MAX CPE value in the DOCSIS configuration file of the cable modem online. **Note** If the value in the configuration file is zero and **no cable modem max-cpe** is configured, then no CPE device is able to obtain an IP address.
Step 4	**cable submgmt default active** **Example:** `Router(config)# cable submgmt default active`	Specifies that the CMTS should actively manage CPE devices. The default is the **no** version of this command, so that the CMTS does not actively manage CPE devices. **Note** This command is required before the Cisco CMTS manages the CPE devices when running a Cisco IOS Release 12.2 BC software image.

	Command or Action	Purpose
Step 5	**cable submgmt default max-cpe** *cpe-num* **Example:** `Router(config)# cable submgmt default max-cpe 4`	(Optional) Specifies the default value for the MAX-CPE parameter that the CMTS should use when the cable modem does not specify a MAX-CPE value in its DOCSIS configuration file.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Note Use of the **cable modem max-cpe unlimited** command can open a security hole in the system by enabling denial of service attacks. It could allow a single user to obtain a large number of IP addresses, and thereby cause the entire network to go down after this single user has reserved all available IP addresses.

Configuring the Maximum Number of Hosts for a Cable Interface

Complete these steps to configure maximum number of hosts for a cable interface:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0`	Enters cable interface configuration mode for the specified cable interface:

	Command or Action	Purpose
Step 4	**cable max-hosts** *number* **Example:** `Router(config-if)# cable max-hosts 10`	Specifies the maximum number of hosts that each cable modem on this cable interface can support.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the Maximum Number of Hosts for a Particular Cable Modem

Complete these steps to configure the maximum number of hosts for a particular cable modem:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cable modem** {*mac-addr* | *ip-addr* } **max-hosts** {*number* | **default**} **Example:** `Router# cable modem 000C.0102.0304 max-hosts 8`	Specifies the maximum number of hosts allowed behind this particular cable modem.

Configuring the Maximum Number of IPv6 addresses for a Cable Modem on the Cisco CMTS

Complete these steps to configure the maximum number of IPv6 addresses for a cable modem in Cisco CMTS:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router> configure terminal`	Enters global configuration mode.
Step 3	**cable modem v6-max-cpe-prefix** [n] **Example:** `Router(config)# cable modem v6-max-cpe-prefix 10`	Specifies the maximum number of IPv6 addresses for a cable modem on the Cisco CMTS for all cable interfaces.
Step 4	**cable submgmt default active** **Example:** `Router(config)#cable submgmt default`	Specifies that the CMTS should actively manage CPE devices. The default is the **no** form of this command, so that the CMTS does not actively manage CPE devices. **Note** This command is required before the Cisco CMTS manages CPE devices when running a Cisco IOS Release 12.2 BC software image.
Step 5	**exit** **Example:** `Router(config)#exit`	Exits global configuration mode.

Configuration Examples for the MAX CPE and Host Parameters

The following example shows how to allow the CMTS to recognize a maximum of four CPE devices attached to online cable modems for a CMTS:

```
cable modem max-cpe 4
```

The following example shows how to set the maximum CPE devices recognized by the CMTS for a cable interface to 15:

```
cable max-hosts 15
```

The following example shows how to allow the CMTS to recognize a maximum of 30 attached CPE devices for a specific cable modem of IP address 172.172.172.12:

```
cable modem 172.172.172.12 max-hosts 30
```

Configuration Examples

To display the current configuration and status of a cable interface, use the **show running-config** command in privileged EXEC mode. The following is sample output that shows that the CMTS permits up to five CPE devices to use the specified cable interface to pass traffic.

```
interface Cable3/0
 ip address 192.168.1.1 255.255.255.0 secondary
 ip address 10.1.1.1 255.255.255.0
 load-interval 30
 no keepalive
 cable max-hosts 5
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 507000000
 cable upstream 0 frequency 27008000
 cable upstream 0 power-level 0
 cable upstream 0 minislot-size 32
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 29008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 4
 no cable upstream 1 shutdown
 cable dhcp-giaddr policy
 cable helper-address 172.17.110.131
end
```

You can also use the **more system:running-config** command to verify the maximum number of permitted CPE devices for a cable interface.

```
CMTS01# more system:running-config
Building configuration...
Current configuration:
!
interface Cable6/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable max-hosts 4
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
```

You can use the **show cable modem detail** command to list information on each CPE device permitted for a cable modem. The command displays the max cpe value as configured in the DOCSIS configuration file for the cable modem, and in parentheses the value of *n* configured in the **cable modem max-cpe** command, if different. See the following sample output where the CMTS is configured for max-cpe equal to four and then max-cpe equal to unlimited:

```
test-cmts# show cable modem detail
```

```
Interface         SID MAC address   Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb    1      yes           37.37
Cable4/0/U0 2      0001.9659.47ab    1      yes           33.70
Cable4/0/U0 3      0001.9659.47bf    1      yes           30.67
Cable4/0/U0 4      0001.9659.3ef7    1      yes           28.84
Cable4/0/U0 5      0001.9659.47eb    1      yes           30.89
test-cmts# conf t
Enter configuration commands, one per line. End with CNTL/Z.
test-cmts(config)# cable modem max-cpe ?
<1-255> Number
unlimited Max CPE not enforced
test-cmts(config)# cable modem max-cpe 4
test-cmts(config)# end
test-cmts#
00:05:11: %SYS-5-CONFIG_I: Configured from console by console
test-cmts# show cable modem detail
Interface        SID MAC address   Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb .1 (4)        yes       37.00
Cable4/0/U0 2      0001.9659.47ab .1 (4)        yes       33.54
Cable4/0/U0 3      0001.9659.47bf .1 (4)        yes       30.70
Cable4/0/U0 4      0001.9659.3ef7 .1 (4)        yes       29.00
Cable4/0/U0 5      0001.9659.47eb .1 (4)        yes       30.92
test-cmts# conf t
Enter configuration commands, one per line. End with CNTL/Z.
test-cmts(config)# cable modem max
test-cmts(config)# cable modem max-cpe ?
<1-255> Number
unlimited Max CPE not enforced
test-cmts(config)# cable modem max-cpe unli
test-cmts(config)# cable modem max-cpe unlimited
test-cmts(config)# ^Z

test-cmts#
00:06:06: %SYS-5-CONFIG_I: Configured from console by console
test-cmts# show cable modem detail
Interface      SID MAC address      Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb   1 (ul)      yes          36.64
Cable4/0/U0 2      0001.9659.47ab   1 (ul)      yes          33.26
Cable4/0/U0 3      0001.9659.47bf   1 (ul)      yes          30.73
Cable4/0/U0 4      0001.9659.3ef7   1 (ul)      yes          29.15
Cable4/0/U0 5      0001.9659.47eb   1 (ul)      yes          30.95
```

Additional References

For additional information related to configuring the MAX CPE and Host parameters on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	Cisco CMTS Cable Command Reference
Interaction of MAX CPE Parameters	Using the max-cpe Command in the DOCSIS and CMTS

Standards

Standards[155]	Title
SP-RFIv1.1-I08-020301	*Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification , version 1.1* (http://www.cablelabs.com/cablemodem/)

155 Not all supported standards are listed.

MIBs

MIBs[156]	MIBs Link
DOCS-CABLE-DEVICE-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

156 Not all supported MIBs are listed.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

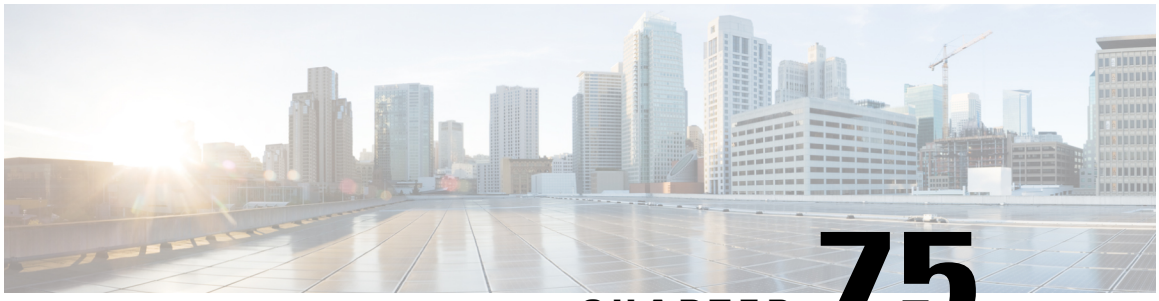
Feature Information for Maximum CPE and Host Parameters for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 212: Feature Information for Maximum CPE and Host Parameters for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.0(6)SC	This feature was introduced on the Cisco uBR7200 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.0(10)SC	The **cable modem max-cpe** command was introduced for the Cisco uBR7200 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.1(2)EC1	This feature was integrated into Cisco IOS Release 12.1(2)EC1.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.1(5)EC	Support was added for the Cisco uBR7100 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.2(4)BC1	This feature was integrated into Cisco IOS Release 12.2(4)BC1 on the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.
TLV63 Support	12.2(33)SCH1	The **cable modem v6-max-cpe-prefix** command was introduced to limit the maximum number of IPv6 addresses per cable modem for the Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.



CHAPTER 75

Power and Thermal Monitoring on the Cisco CMTS Routers

First Published: May 10, 2010

The power and thermal monitoring feature provides monitoring options for the thermal and power consumption of the Cisco UBR-MC20X20V cable interface line card.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Power and Thermal Monitoring

The table shows the hardware compatibility prerequisites for this feature.

Table 213: Power and Thermal Monitoring for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCD2 and later • PRE4	Cisco IOS Release 12.2(33)SCD2 and later • Cisco UBR-MC20X20V[157]

157 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

Note Any reference to the Cisco UBR-MC20X20V cable interface line card used in this document is also applicable to its three variants—Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D.

- The Cisco UBR10012 universal broadband router must be running Cisco IOS 12.2(33)SCD2 release or later.

Restrictions for Power and Thermal Monitoring

The Power and Thermal Monitoring feature has the following restrictions and limitations:

- The power and thermal monitoring facility is enabled by default and you cannot disable it.
- The thermal thresholds are predefined and you cannot configure or modify them.

Information About Power and Thermal Monitoring

The power and thermal monitoring feature provides monitoring options for the thermal and power consumption of the Cisco UBR-MC20X20V cable interface line card. The power and thermal monitoring facility monitors the line card at several different points (See Table 214: Thermal Thresholds for the Cisco UBR-MC20X20V Line Card) to see whether it is overheating or drawing too much power.

The monitoring facility triggers an alert when the operational thresholds are exceeded. Alerts are in the form of syslog messages, alarms, and SNMP traps. Syslog messages are generated when the temperature sensors cross their respective thermal threshold levels. Alarms and SNMP traps are generated only when the inlet sensors cross their thresholds. In addition to the alerts, the power consumption of the line card is checked periodically by the monitoring facility.

The following sections describe the Power and Thermal Monitoring feature in more detail:

Thermal Monitoring

The thermal monitoring facility uses temperature sensors, placed at several different points in the line card, to monitor the thermal threshold levels. Each temperature sensor is monitored against the thermal threshold levels that are specific to the sensor.

The table shows the sensors monitored and their corresponding thresholds.

Note The thermal thresholds shown in the table are predefined and you cannot configure or modify them.

Table 214: Thermal Thresholds for the Cisco UBR-MC20X20V Line Card

Sensor	Minor Threshold (in Celsius)	Major Threshold (in Celsius)	Critical Threshold (in Celsius)
Nickel 10G	82	87	92
CPU	73	78	83
Inlet	68	73	78
Remora	82	87	92
Coldplay	75	80	85
Waxbill	92	97	102
Fauna	82	87	92
Flora	80	85	90
Toucan FPGA A	94	97	100
Toucan FPGA B	94	97	100
Toucan FPGA C	94	97	100

The Cisco UBR-MC20X20V cable interface line card thermal monitoring has three levels of monitoring thresholds: Minor, Major, and Critical. The table shows the thresholding states and their corresponding descriptions.

Table 215: Thresholding States for the Cisco UBR-MC20X20V Line Card

State	Description
Minor	The temperature sensor moves to minor state when the sensor readings stay constant for 2 minutes between minor and major (>= minor and < major) thresholds.
Major	The temperature sensor moves to major state when the sensor readings stay constant for 2 minutes between major and critical (>= major and < critical) thresholds.
Critical	The temperature sensor moves to critical state when the sensor readings stay above the critical (>= critical) threshold.

The temperature sensors are monitored every 2 minutes, with a soaking interval (A soaking interval defines how long a condition must persist before an alarm is declared.) of 2 minutes for minor and major events; there is no soaking interval for critical events.

The following alerts are generated on the Cisco UBR-MC20X20V cable interface line card:

- A syslog error message is generated when a thermal threshold is broken. The syslog error message contains sensor name, reading, threshold state, value, event timestamp, and card power level.
- Alarms and SNMP traps are generated when the inlet sensor crosses its threshold.

Note A high availability (HA) switchover is not initiated for the Cisco UBR-MC20X20V cable interface line card when the temperature sensors cross the critical threshold.

The temperature history of the router is maintained for an hour, with timestamp. It can be viewed using the show environment command. The show environment command displays the PRE temperature, fan status, power supply details, and the thermal and power status of the line card. The slot/subslot option of the show environment command helps to identify the location of the line card.

The thermal monitoring data is exclusive to the Cisco UBR-MC20X20V cable interface line card. When the line card is reset or removed, the outstanding temperature alarm is cleared. However, you can still view the temperature history of the line card that was maintained by the OBFL feature using the show logging onboard slotindex temperature command.

In the event of a line card crash, the temperature history of the line card is viewable from the crashinfo file. The crashinfo file contains the temperature history of the line card for the last one hour before the crash. The data is displayed using the show logging onboard command. See the Onboard Failure Logging feature guide for more details.

A PRE switchover does not impact the monitoring functionality of the line card. All the outstanding temperature threshold alarms are retained.

Power Monitoring

The following power monitoring options are implemented on the Cisco UBR-MC20X20V cable interface line card:

- The power consumption is monitored every 2 minutes.
- The power consumption history of the line card is maintained for an hour, with timestamp. You can view it using the show environment command.

The power consumption history of the line card is not maintained after an OIR; the history is erased and it cannot be retrieved. However, in case of a line card crash, the power consumption history of the line card is available from the crash log file for the last one hour before the crash. The syslog error message also captures the line card power consumption details at the time of the thermal threshold breach.

Alerts

The thermal and power monitoring feature triggers an alert when the operational thresholds are exceeded.

The Cisco uBR10012 universal broadband router uses the following types of alerts:

- Alarms
- SNMP Traps
- Syslog Messages

Alarms

The monitoring facility triggers an alarm when the inlet sensor of the Cisco UBR-MC20X20V cable interface line card breaches a predefined thermal threshold. The temperature status of the line card is maintained by the RP in Cisco uBR10012 universal broadband router. When the temperature varies, the line card passes the information to the RP to fire an alarm and SNMP trap. The RP clears the current outstanding temperature alarm and generates a new alarm. You can view these alarms using the show facility alarm status command.

SNMP Traps

SNMP traps are generated when the inlet temperature sensor of the Cisco UBR-MC20X20V cable interface line card has a status change among normal, minor, major or critical. You can view the SNMP traps through the SNMP manager. To disable SNMP traps, use the no form of the snmp-server enable traps envmon [temperature] command.

The following MIBs are used to generate SNMP traps when the line card crosses thermal thresholds:

- ciscoEnvMonTempStatusChangeNotif: This SNMP trap is generated when the inlet temperature status changes among normal, minor, major or critical.
- ciscoEnvMonTemperatureNotification: This SNMP trap is generated when the inlet temperature status changes from normal to minor, major or critical.

The following is a sample SNMP trap output from SNMP Manager:

```
Received SNMPv2c Trap:
Community: public
```

```
From: 10.11.0.17
mib_2.1.3.0 = 500023
internet.6.3.1.1.4.1.0 = ciscoEnvMonTempStatusChangeNotif
ciscoEnvMonTemperatureStatusDescr.6 = Inlet SubSlot 6/1
ciscoEnvMonTemperatureStatusValue.6 = 70
ciscoEnvMonTemperatureState.6 = warning(2)
Received SNMPv2c Trap:
Community: public
From: 10.11.0.17
mib_2.1.3.0 = 500023
internet.6.3.1.1.4.1.0 = ciscoEnvMonTemperatureNotification
ciscoEnvMonTemperatureStatusDescr.6 = Inlet SubSlot 6/1
ciscoEnvMonTemperatureStatusValue.6 = 70
ciscoEnvMonTemperatureState.6 = warning(2)
```

Syslog Messages

Syslog error messages are generated when the temperature sensor of the Cisco UBR-MC20X20V cable interface line card crosses a thermal threshold. The syslog error message also contains the power consumption level of the line card during the time of thermal threshold crossover event.

The following is a sample syslog error message output:

```
SLOT 6/1: Apr  6 19:08:02.584: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: CPU temperature MINOR
limit (73 degC) exceeded at temperature 74 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:50:02.652: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Nickel 10G temperature
 MINOR limit (82 degC) exceeded at temperature 83 degC and power 172.897 watts
SLOT 6/1: Apr  6 19:50:04.152: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Waxbill temperature
MINOR limit (92 degC) exceeded at temperature 93 degC and power 172.897 watts
SLOT 6/1: Apr  6 19:58:04.168: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Remora temperature MINOR
 limit (82 degC) exceeded at temperature 83 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:05.668: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Coldplay temperature
MINOR limit (75 degC) exceeded at temperature 75 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:07.168: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Fauna temperature MINOR
 limit (82 degC) exceeded at temperature 83 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:08.668: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Flora temperature MINOR
 limit (80 degC) exceeded at temperature 81 degC and power 172.217 watts
```

How to Configure Power and Thermal Monitoring

This section contains the following procedure:

Power and Thermal Monitoring Configuration

The power and thermal monitoring facility for the Cisco UBR-MC20X20V cable interface line card is enabled by default and you cannot disable it. However, you can disable the facility alarms using the no form of the facility-alarm command. Similarly, you can use the no form of the snmp-server enable traps envmon [temperature] command to disable SNMP traps.

Monitoring Power and Thermal Information

To monitor the Power and Thermal Monitoring facility, use the following procedures:

Viewing Thermal and Power Information

To view information about the power and thermal monitoring of the Cisco UBR-MC20X20 cable interface line card, use the **show environment** command in privileged EXEC mode.

For a complete description of the command, see the Cisco IOS Cable Command Reference Guide on Cisco.com.

Example

The following example shows a typical display for the **show environment** command.

```
Router# show environment subslot 7/0
------------------------------------------------------------------------
TEMPERATURE/POWER INFORMATION
------------------------------------------------------------------------
Number of Temperature Sensors : 11
Sampling frequency            : 2 minutes
------------------------------------------------------------------------
Sensor       | ID | Current     | Minor | Major | Critical | Alarm     |
             |    | Temperature |       Threshold          | Condition |
             |    |     0C      |          0C              |           |
------------------------------------------------------------------------
Nickel 10G     1       48          82    87      92        Normal
Inlet #1       2       36          68    73      78        Normal
CPU            3       44          73    78      83        Normal
Remora         4       48          82    87      92        Normal
Coldplay       5       40          75    80      85        Normal
Waxbill        6       53          92    97      102       Normal
Fauna          7       46          82    87      92        Normal
Flora          8       47          80    85      90        Normal
Toucan FPGA A  9       45          94    97      100       Normal
Toucan FPGA B  10      36          94    97      100       Normal
Toucan FPGA C  11      47          94    97      100       Normal
------------------------------------------------------------------------
Power: 168.813 watts
------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
       Time Stamp       |  Power  |  Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS     |  watts  |  1    2    3    4    5    6    7    8    9   10   11
------------------------------------------------------------------------------------------------
09/30/2009 10:24:26       168.813    48   36   44   48   40   53   46   47  45   36   47
09/30/2009 10:22:26       168.813    48   36   44   48   40   53   46   47  45   36   47
09/30/2009 10:20:26       168.813    48   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:18:26       168.813    48   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:16:26       168.813    47   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:14:26       168.813    47   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:12:26       168.813    47   36   44   46   40   52   45   47  45   36   47
09/30/2009 10:10:26       168.813    47   35   44   45   39   51   45   47  45   36   47
09/30/2009 10:08:26       168.132    46   35   44   43   38   50   43   47  45   36   47
------------------------------------------------------------------------------------------------
```

Viewing Thermal and Power Monitoring Alarms

To view the power and thermal monitoring alarms of the Cisco UBR-MC20X20 cable interface line card, use the show facility-alarm status command in privileged EXEC mode.

For a complete description of the command, see the Cisco IOS Cable Command Reference Guide on Cisco.com.

Example

The following example shows a typical display for the **show facility-alarm status** command.

```
Router# show facility-alarm status
Thresholds:
Intake minor 45 major 54 critical 67
Outlet minor 48 major 58 critical 85
System Totals  Critical: 1  Major: 1  Minor: 1
Source              Severity      ACO         Description [Index]
------              --------      ---         -------------------
chassis             MINOR         NORMAL      Subslot 7/0 Inlet temperature limit
chassis             MAJOR         NORMAL      Subslot 7/1 Inlet temperature limit
chassis             CRITICAL      NORMAL      Subslot 8/0 Inlet temperature limit
```

Additional References

The following sections provide references related to the Power and Thermal Monitoring feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Onboard Failure Logging	Onboard Failure Logging
Cisco Cisco UBR-MC20X20V Cable Interface Line Card Hardware Installation Guide	Cisco UBR-MC20X20V Cable Interface Line Card Hardware Installation Guide

Standards

Standards	Title
None	—

MIBs

MIBs[158]	MIBs Link
• CISCO-ENVMON-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

158 Not all supported MIBs are listed.

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Power and Thermal Monitoring on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 216: Feature Information for Power and Thermal Monitoring on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Power and Thermal Monitoring	12.2(33)SCD2	The Power and Thermal Monitoring feature was introduced for the Cisco UBR-MC20X20V line card. The following section provides information about this feature: The following command was modified: • **show environment**

CHAPTER 76

PXF Divert Rate Limit Enhancement on the Cisco CMTS Routers

First Published: December 18, 2008

Last Updated: January 28, 2016

This document describes the Parallel eXpress Forwarding (PXF) Divert Rate Limit (DRL) Enhancement on the Cisco Cable Modem Termination System (CMTS). This feature prevents congestion of packets on the forwarding processor (FP) or the PXF processor to the Route Processor (RP) interface, which can be caused by denial of service (DoS) attacks directed at the CMTS or by faulty hardware.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for PXF DRL Enhancement

The PXF DRL Enhancement feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2(33)SCB. The table shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 217: PXF DRL Enhancement Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later** • PRE2	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [159]

159 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

Restrictions for PXF DRL Enhancement

- DRL cannot be configured on a cable bundle interface.
- The trusted-site list can contain a maximum of four sites.
- WAN-IP entities are identified using a hash, and hash collisions can occur between two (or more) entities.
- The DRL feature is always on; it cannot be turned off.
- The PXF DRL Enhancement feature is not applicable to Address Resolution Protocol (ARP) packets arriving from a cable interface. These packets are rate limited by the ARP filter feature.

Information About PXF DRL Enhancement

The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion.

Diverted packets are sent from the forwarding processor to the Route Processor through the FP-to-RP interface. This interface gets congested when packets (that require diversion) arrive at the FP at a faster rate than they can be transmitted to the RP. When the interface gets congested, valid packets in the FP-to-RP queues are tail-dropped. This situation can be caused deliberately by DoS attacks directed at the CMTS, or by faulty external hardware.

The PXF DRL Enhancement feature identifies packet streams that cause congestion on the FP-to-RP interface. Packets in the stream are then dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, thereby allowing other valid packets to reach the RP.

The PXF DRL Enhancement feature applies to both cable and WAN interfaces.

Even if the DRL (per source based divert rate limit) is configured on the WAN interface, sometimes the RP gets overloaded due to Distributed Dos (DDos) attack. The DDos attack is seen when the following occurs:

- When the packets are being pointed to the CMTS directly.
- When the packets are being pointed to a CPE. If the CPE goes down and all traffic gets punted to PRE.

Effective with Cisco IOS Release 12.2(33)SCH3, when the DDos occurs and the flooding packets have one of the support divert codes, the DRL Max-Rate Per Divert-Code on WAN Interface can be configured to reduce the CPU utilization.

PXF DRL Enhancement on a Cable Interface

The PXF DRL Enhancement feature applies to upstream packets from a cable interface. In cable, the entities must be rate-limited on a deterministic basis. Because certain entities (for example, VoIP calls) must be able to divert packets successfully, a probabilistic model cannot be used. As a result, the Media Access Control (MAC)-domain and service identifier (SID) identifies the subscribers. DRL aggregates and limits all diverted traffic originating from a subscriber.

PXF DRL Enhancement on a WAN Interface

The PXF DRL Enhancement feature applies to packets from a non-cable interface (typically a Gigabit Ethernet line card.) WAN-side entities cannot be rate-limited on a deterministic basis due to the large number of entities that can exist. Therefore, a probabilistic model (that is, a hash) is used to identify packet streams. This means that not all entities will be uniquely identified.

IP packet streams are identified and rate-limited by a hash of the source IP address, the fib-root (for example, the VPN routing and forwarding [VRF] name), and the divert code. Non-IP packet streams are not expected on the WAN interface, and are therefore rate-limited on a divert code basis.

A WAN-side “trusted-site” list can be maintained, with a maximum of four trusted sites. Each entry in the “trusted-site” list contains an IP address and mask, an IP type of service (ToS) value and mask, and a VRF name. Packets matching a trusted site will not be subject to rate-limiting. In addition, packets from trusted sites will not affect the rate-limiting of packets from other entities.

How to Configure PXF DRL Enhancement on the Cisco CMTS Routers

This section describes the following required and optional procedures:

Configuring US Cable Divert-Rate-Limit

The cable side DRL is configured on the physical cable interface. It cannot be configured on a cable bundle interface. To configure cable DRL, use the **cable divert-rate-limit** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface* **Example:** `Router(config)# interface C5/0/0`	Enters interface configuration mode for the specified interface. • **interface—**Specifies the name of the physical Cable interface.
Step 4	**cable divert-rate-limit rate** *rate* **limit** *limit* **Example:** `Router(config-if)#` **cable divert-rate-limit rate 1 limit 4**	Specifies the DRL rate and limit. • **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. The default rate is 2000 packets per second. • **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. The default limit is 2000 packets.
Step 5	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv4 Rate and Limit

To configure DRL for WAN-side IPv4 packet streams, use the **service divert-rate-limit ip** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit ip** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **service divert-rate-limit ip fib-rp-glean rate 1 limit 4**	Specifies the DRL rate and limit for the WAN interface. • **divert-code—**Specifies the applicable divert code. • **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv6 Rate and Limit

To configure DRL for WAN-side IPv6 packet streams, use the **service divert-rate-limit ipv6** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit ipv6** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10`	Specifies the DRL rate and limit for the WAN interface. • *divert-code*—Applicable divert code. Refer to the list of divert codes in Cisco IOS CMTS Cable Command Reference • **rate**—Divert rate in packets per second. The minimum rate is 1 packet per second and the maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit**—Number of packets to be diverted in an initial burst of packets. The minimum limit is 4 packets and the maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Non-IP Rate and Limit

To configure DRL for WAN-side non-IP packet streams, use the **service divert-rate-limit non-ip** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit non-ip** *divert-code* **rate** *rate* **limit** *limit*	Specifies the DRL rate and limit for the WAN interface. • **divert-code**—Applicable divert code.

	Command or Action	Purpose
	Example: `Router(config)# service divert-rate-limit non-ip cgmp rate 1 limit 4` **Example:**	• **rate—**Divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN non-IP packets, the default rate is 2000 packets per second. • **limit—**Number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN non-IP packets, the default limit is 2000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv4 Trusted Site

Each entry in the IPv4 trusted-site list contains a source IP address and mask, an IP ToS value and mask, and a VRF name. The IPv4 "trusted-site" list applies only to WAN-side IPv4 packets. A maximum of four IPv4 trusted sites can be configured.

To configure a trusted-site list, use the **service divert-rate-limit trusted-site** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **Example:** **Example:** **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **global**	Adds entries to the IPv4 trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet. • **source-ip—**Specifies the source IP address that should be matched.

	Command or Action	Purpose
	Example: **Example:** **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **vrf** *vrf-name* **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 global** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 vrf name1**	• **ip-mask—**Specifies the mask to apply to the source IP address of the packet before testing if it matches. There are no restrictions on the mask-ip-address value. • **tos tos-value—**Specifies the ToS value of the trusted site. There are no restrictions on the tos-value value. • **mask tos-mask—**Specifies the mask to apply to the IP ToS value and the trusted-site tos value before testing whether it matches. There are no restrictions on the tos-mask value. • **global—**Specifies that the trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name—**Specifies the VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the IPv4 trusted site list.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv6 Trusted Site

Each entry in the IPv6 'trusted site' list contains a 128-bit source IP address & mask, an 8-bit traffic-class value & mask, and a VRF name. The IPv6 trusted-site list applies only to WAN-side IPv6 packets. A maximum of four IPv6 trusted site can be configured.

To configure a IPv6 trusted-site list, use the service divert-rate-limit trusted-site-ipv6 command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **global** **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **vrf** *vrf-name* **Example:** `Router(config)#service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class 0x3 mask 0xFF global`	Adds IPv6-specific entries to the trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet. • ip-address/prefix-length—The source IPv6 address/ prefix-length that should be matched. • traffic-class tc_value—The 8-bit traffic-class of the trusted site. There are no restrictions on the tc_value. • mask tc-mask—The mask to apply to the packet traffic-class and the trusted-site tc_value before testing if it matches. • **global**—The trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name**—VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the trusted site list.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on WAN Interface

Effective with Cisco IOS Release 12.2(33)SCH3, per-divert-code rate limit can be configured on the WAN interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on WAN Interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the WAN interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit max-rate wan** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100`	Specifies the DRL rate and limit for the WAN interface per divert-code. • **divert-code—**Specifies the applicable divert code. ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving. Starting from Cisco IOS Release 12.2(33)SCJ, the following divert codes were supported: ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet

	Command or Action	Purpose
		◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. • **rate**—Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit**—Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on Upstream Cable Interface

Effective with Cisco IOS Release 12.2(33)SCJ, per-divert-code rate limit can be configured on the upstream cable interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on upstream cable interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the upstream cable interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit max-rate us-cable** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100`	Specifies the DRL rate and limit for the upstream cable interface per divert-code. • **divert-code—**Specifies the applicable divert code. ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet ◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ src_ver_leasequery_req—Divert to RP due to zero MD and sid value and need to send lease query to DHCP server for those packets. ◦ src_ver_unknown_ip_addr—Divert to RP due to zero MD and sid value and no adjacency information for source IP address of those packets. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ ipv6_src_ver_mac_req—Divert to RP due to zero MD and sid value.

	Command or Action	Purpose
		• **rate—**Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit—**Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying US Cable Dropped Packets

To view and verify the number of upstream cable packets that are dropped from the CMTS, use the show pxf cpu statistics drl us-cable command as shown in the following examples:

```
Router# show pxf cpu statistics drl us-cable
Divert-Rate-Limit US-cable statistics
   dropped   identifier
       361   interface: Cable6/0/1   SID: 28
      2457   interface: Cable6/0/0   SID: 1
Router# show pxf cpu statistics drl us-cable threshold 400
Divert-Rate-Limit US-cable statistics :: threshold = 400
   dropped   identifier
      2457   interface: Cable6/0/0   SID: 1
Router#
```

Verifying WAN IPv4 Dropped Packets

To verify drop counters for WAN-IPv4 packets, use the show pxf cpu statistics drl ipv4 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv4
Divert-Rate-Limit WAN-IPv4 statistics
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
       150   11.12.13.10  VRF: global  divert_code: fib_limited_broadcast
Router#
Router# show pxf cpu statistics drl ipv4 threshold 400
Divert-Rate-Limit WAN-IPv4 statistics :: threshold = 400
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
```

Verifying WAN IPv6 Dropped Packets

To verify drop counters for WAN-IPv6 packets, use the show pxf cpu statistics drl ipv6 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv6
```

```
Divert-Rate-Limit WAN-IPv6 statistics
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
       150   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_punt
Router#
Router# show pxf cpu statistics drl ipv6 threshold 400
Divert-Rate-Limit Cable/WAN-IP statistics :: threshold = 400
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
Router#
```

Verifying WAN Non-IP Dropped Packets

To verify drop counters for WAN non-IP packets, use the **show pxf cpu statistics drl non-ip or** show pxf cpu statistics drl non-ip threshold commands as shown in the following examples:

```
Router# show pxf cpu statistics drl non-ip
Divert-Rate-Limit WAN-non-IP statistics
   dropped divert_code
         5 cdp
        17 cgmp
Router# show pxf cpu statistics drl non-ip threshold 10
Divert-Rate-Limit WAN-non-IP statistics :: threshold = 10
   dropped divert_code
        17 cgmp
```

Verifying the Trusted-Site List

To verify the trusted-site configuration, use the **show pxf cpu drl trusted-sites** command as shown in the following example:

```
Router# show pxf cpu drl trusted-sites
Divert-Rate-Limit IPv4 Trusted-Site list
 IP-addr          IP-addr mask     ToS   ToS mask  VRF
 60.0.1.0         255.255.255.0    0x18  0xF8      blue
 50.0.1.0         255.255.255.240  0x01  0xFF      <all>
 50.0.0.0         255.255.255.0    0x18  0xF8      <global internet>
Divert-Rate-Limit IPv6 Trusted-Site list
 5436:6AB4:2344::1/128  tc 0xA3  tc_mask 0xFF  VRF <all>
Router#
```

Verifying WAN DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the WAN interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu  statistics drl max-rate wan threshold 1
dropped   divert_code
      2617    cable_filter_us
```

Verifying US Cable DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the US cable interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu statistics drl max-rate us-cable
Load for five secs: 44%/4%; one minute: 45%; five minutes: 28%
Time source is hardware calendar, 16:52:36.953 CST Thu Dec 17 2015
```

```
Divert-Rate-Limit max-rate US-cable statistics
   dropped   divert_code
 No max-rate US-cable drops.
```

Clearing Statistics

Use **clear** commands to do the tasks listed in the table:

Command	Description
clear pxf statistics drl all	To clear all the entries in all the DRL statistics table
clear pxf statistics drl us-cable	To clear all the entries in the US-cable statistics table
clear pxf statistics drl ipv4	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl ipv6	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl non-ip	To clear all the entries in the WAN non-IP statistics table
clear pxf statistics drl max-rate	Clears the DRL max-rate statistics on the WAN interface

Note Starting from Cisco IOS Release 12.2(33)SCJ, only the **clear pxf statistics drl all** command is supported.

Configuration Examples for PXF DRL Enhancement

This section provides the following configuration examples:

Example: Configuring Cable Divert Rate Limit

The following example shows how to configure a cable DRL.

```
Router(config)# interface C5/0/0
Router(config-if)#cable divert-rate-limit rate 1 limit 4
```

Example: Configuring WAN IPv4 Rate and Limit

The following example shows how to configure a WAN-IPv4 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ip
service divert-rate-limit ip fib_rp_glean
```

```
service divert-rate-limit ip fib_rp_glean rate
service divert-rate-limit ip fib_rp_glean rate 65530
service divert-rate-limit ip fib_rp_glean rate 65530 limit
service divert-rate-limit ip fib_rp_glean rate 65530 limit 4194
```

Example: Configuring WAN IPv6 Rate and Limit

The following example shows how to configure a WAN-IPv6 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ipv6
service divert-rate-limit ipv6 ipv6_rp_glean
service divert-rate-limit ipv6 ipv6_rp_glean rate
service divert-rate-limit ipv6 ipv6_rp_glean rate 20
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10
```

Example: Configuring WAN Non-IP Rate and Limit

The following example shows how to configure a WAN Non-IP rate and limit.

```
service divert-rate-limit
service divert-rate-limit non-ip
service divert-rate-limit non-ip cgmp
service divert-rate-limit non-ip cgmp rate
service divert-rate-limit non-ip cgmp rate 65535
service divert-rate-limit non-ip cgmp rate 65535 limit
service divert-rate-limit non-ip cgmp rate 65535 limit 4100
```

Example: Configuring an IPv4 Trusted Site

The following example shows how to configure an IPv4 trusted site.

```
service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255
  tos 0xD0 mask 0xF3
```

Example: Configuring an IPv6 Trusted Site

The following example shows how to configure a IPv6 trusted site.

```
service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class
 0x3 mask 0xFF global
```

Example: Configuring DRL Max-Rate Per Divert-Code on WAN Interface

The following example shows how to configure DRL max-rate per divert-code on WAN interface

```
Router> enable
Router# configure terminal
Router(config)# service  divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Example: Configuring DRL Max-Rate Per Divert-Code on US Cable Interface

The following example shows how to configure DRL max-rate per divert-code on upstream cable interface.

```
Router> enable
Router# configure terminal
Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Additional References

The following sections provide references related to the PXF Divert Rate Limit Enhancement feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Cable ARP Filtering	Cisco IOS CMTS Cable Software Configuration Guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PXF DRL Enhancement

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

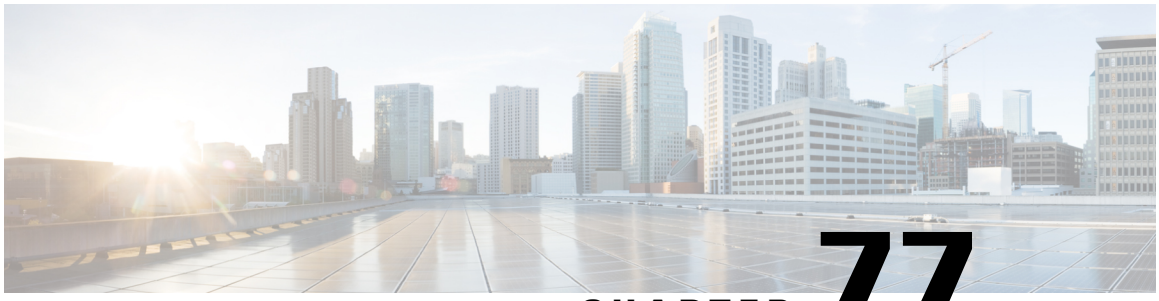
Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 218: Feature Information for PXF DRL Enhancement

Feature Name	Releases	Feature Information
PXF DRL Enhancement on the Cisco CMTS Routers	12.2(33)SCB	The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion. The following sections provide information about this feature: The following commands were introduced or modified: cable divert-rate-limit, • **service serviceip** • **service servicenon-ip** • **service divert-rate-limit trusted-site** • **clear pxf statistics drl cable-wan-ip** • **show pxf cpu statistics**, **show pxf cpu drl-trusted-sites**

Feature Name	Releases	Feature Information
PxF Accelerated for IPv6 Forwarding	12.2(33)SCE	The PXF Accelerated for IPv6 Forwarding feature for the Cisco uBR10000 series router includes support for the following IPv6 features: • IPv6 Security and QoS ACLs • IPv6 over IPv4 Tunnels • IPv6 Packet Filter Groups • IPv6 QoS Classifiers • ToS Overwrite for IPv6 • IPv6 Source Verify • IPv6 Packet Intercept • IPv6 SAV The following commands were introduced: service divert-rate-limit trusted-site-ipv6, **service divert-rate-limit ipv6,** show pxf cpu statistics drl us-cable, show pxf cpu statistics drl ipv6, show pxf cpu statistics drl ipv4, and **show pxf cpu statistics drl non-ip**.
DDoS attack solution	12.2(33)SCH3	The DDOS attack solution feature helps reduce the CPU utilization when the DDos occurs. The following commands were introduced: • **service divert-rate-limit max-rate** • **clear pxf statistics drl max-rate** • **show pxf cpu statistics drlmax-rate**

Feature Name	Releases	Feature Information
IPv6 DRL Punt Codes	12.2(33)SCJ	The feature applies rate limit to traffic from upstream cable. The following commands were introduced: • **service divert-rate-limit max-rate us-cable** • **show pfx cpu statistics drl max-rate us-cable** • **clear pfx statistics drl all**



CHAPTER 77

Resolving Common Image Installation Problems

Note The information in this document is based on Cisco IOS Release 11.2 and later releases.

This appendix is designed to assist you with problems that may develop while you are installing Cisco IOS software images using a TFTP or remote copy protocol (rcp) server application. For rcp applications, substitute rcp for TFTP in the instructions.

Contents

Before You Begin

Caution Do not save anything while you are in boot mode. Avoid using the saving commands (write mem or copy run start), and respond **no** to any prompt suggesting that you save your current configuration. If you save while you are in this mode, your configuration can be partially or completely erased.

Resolving Default Gateway Issues

Determine the Default Gateway for the Router

The default gateway is always the next hop that any packet will have to cross to reach the workstation where you have the TFTP server or Telnet session source, or both. The traceroute command shows the IP address of the default gateway in the first line of the output:

Example

```
Router> traceroute 172.17.247.195
Type escape sequence to abort.
Tracing the route to 172.17.247.195
1 10.200.40.1 4 msec 4 msec 4 msec
2 172.17.247.195 4 msec *  0 msec
Router>
```

Adding the Default Gateway in the Configuration

To add the default gateway, type the **ip default-gateway** command in the global configuration mode.

```
ip default-gateway [ip address]
```

ip address	The IP address of the router.

Verifying the TFTP Server and Router are in the Same Network

You will need to compare the IP addresses and masks of the TFTP server and the Ethernet interface of the router.

Example 1

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.17.3.192 and the mask is 255.255.0.0. In this example, the TFTP server and this interface of the router are in the same network, so a default gateway is not required.

Example 2

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.10.3.192 and the mask is 255.255.0.0. In this example, they are on different IP networks so it is necessary to configure a default gateway on the router.

Determining the IP Address and Mask on the Router

Look for the IP address command under the interface Ethernet statement in your configuration.

Example

```
Router> en
Password:
Router# show run
Building configuration...
Current configuration:
!
version 11.3
service timestamps debug uptime
.....................
interface Ethernet0
ip address 172.17.3.192 255.255.0.0
```

Determining the IP Address of the TFTP Server on Windows 95

Step 1 From the toolbar, select Start and then Run.

Step 2 Type winipcfg and then click OK to display the IP configuration dialog box.

Determining the IP Address of the TFTP Server on a UNIX Workstation

Step 1 Enter the command netstat -in. The IP addresses of the interfaces on your station appear.

Step 2 Select the IP address for the interface that goes into the router network.

Troubleshooting Problems During Software Transfer

Resolving Error Message Text checksum verification failure During the Copy

If you have seen many "." instead of "!" during the copy, you may see a message similar to the following example:

```
COPY: Text checksum verification failure
TFTP from 172.17.247.195 failed/aborted
Verifying checksum... invalid (expected 0x62B7,
computed 0x60B9)
```

If you enter a show flash command, you may see something similar to the following example:

```
Router# show flash
PCMCIA flash directory:
File Length Name/status
1 3437967 c1600-sy-mz.120-8.0.2.T
2 3489036 c1600-y-l.112-19.P1
3 290304 c1600-y-l.112-18.P [invalid checksum]
```

In both cases, a checksum failure indicates that the file has not been properly copied into the memory and you need to copy it again. First, verify that the file you copied to the TFTP server is the same size as the original file. (Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.) If the network is very busy, you may also see this behavior; try the copy again when the network is not so loaded, or establish a direct Ethernet connection between the TFTP server and the router to download the file.

Resolving Error Message "error opening tftp"

This is an example of the error message:

```
Router# copy tftp flash
Address or name of remote host [172.17.0.5]?
Source filename [rsp-dsv-mz.112-19.P1.bin]?
Destination filename [rsp-dsv-mz.112-19.P1.bin]?
Accessing tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin...
%Error opening tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin (No such file or directory)
```

If you receive this message, verify that the file is in the root directory of the TFTP server, and check to see if you entered the correct filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

Resolving Display of Timeout Error Messages

Step 1 Verify that the TFTP server is open on your PC.

Step 2 Make sure that the file is in the root directory (from the menu bar, select **View**>**Options**).

Resolving Error Message "Can't open file"

Verify that the TFTP server is running on your PC. Verify that you have copied the exact filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

Instructions for Run-from-RAM Installations

Step 1 To copy a system image from one device to another, use the copy command in global configuration mode.

Example:

```
copy tftp ?
```

Step 2 Refer to the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 for additional information about the copy command. Methods vary according to different platforms.

What to Do Next

The three most common forms of the copy command for this purpose are as follows:

```
copy tftp flash
copy rcp flash
copy slot0: slot1:
```

The following example provides an illustration of the copy slot0: slot1 command:

```
router# show slot0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
```

```
name
1 .D unknown 5E8B84E6 209D8 11 2392 Jan 22 2000 00:22:42
flashconfig
2 .. image 5E7BAE19 B623C4 22 11802988 Jan 22 2000 00:23:18
rsp-jsv-mz.1
20-8.0.2.T
router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
name
1 .. unknown 6A2B4BA7 6FA9E0 20 7186784 Jul 30 1999 15:05:19
rsp-jv-mz.11 1-26.CC1
2 .. config 631F0D8B 6FB1EC 6 1929 Oct 19 1999 06:15:49
config
     3 .. config 631F0D8B 6FB9F8 7 1929 Oct 19 1999 06:16:03
     config1
router# copy slot0: slot1:
Source filename []? rsp-jsv-mz.120-8.0.2.T
Destination [slot1]?
CCCCCCCCCCCCCCCCCCC
2392 bytes copied in 0.300 secs
```

Instructions Before Reloading

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you must start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

What to Do Next

This is an example of boot system commands defined in the configuration file:

```
Router> en
Password:
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)# boot system flash c1600-y-l.112-18.P
Router(config)# boot system flash
```

Troubleshooting Problems by Verifying the Software Image

Resolving the show version Command not Displaying Proper Image

If the show version command output does not display the Cisco IOS image that you just loaded, perform these steps:

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

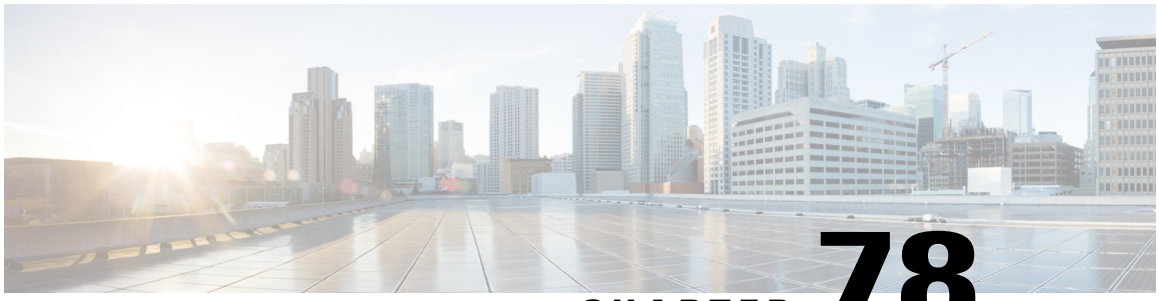
Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

Resolving the Rxboot Prompt (Router(boot)) Displaying After Reload

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

Step 3 Verify that the config register value is correct. The last digit should be a 2. You can check this with the show version command. If the value is not correct, you need to restore a valid value and reload the image.



CHAPTER 78

SEA Health Monitoring for the Cisco UBR10012 Routers

First Published: November 16, 2009

Last Updated: November 16, 2009

Maintaining a log of major and critical events and alarms helps the system administrator in identifying and resolving the problems from further occurrence. There are various other methods for reproducing the problems but these methods have limitations. The System Event Archive (SEA) is a health monitoring feature. It maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. The SEA feature maintains a log of hardware and software events and alarms in the sea_log.dat file. These generated events can be analyzed and copied to the sea_log.dat file at the specified location. The Cisco IOS Release 12.2(33)SCC introduces the SEA feature for Cisco Universal Broadband Router 10012.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for SEA

The table shows the hardware and software compatibility prerequisites for this feature.

Table 219: SEA Support for the Cisco CMTS Routers Hardware and Software Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards or Jacket Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[160] **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[161] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2	• Cisco Wideband SPA 2

160 Supports DOCSIS 2.0 and IPv6 cable modems.
161 Supports DOCSIS 3.0 and IPv6 cable modems.

Restrictions for SEA

- SEA event log feature only supports PCMCIA ATA disk or Compact flash disk in adapter for PRE2.
- Due to a limitation (reference CDETS ID: CSCsz77977) for performing Online-Insertion-Removal (OIR) of the disk on PRE2, the following actions are recommended before performing an OIR of the disk on PRE2:
- Disable SEA logging using **no logging system** command, before performing an OIR of disk on PRE2.
- Enable SEA logging using **logging system** command, after performing OIR of disk on PRE2.
- Use different disk for SEA logging and for storing Cisco IOS image. For example, if disk0: is used to store IOS image and is referenced in boot system command, use disk1: for storing SEA logging.
- For PRE4, keep the SEA storage on boot flash: (which is the default disk).

Information About SEA

The following sections provide the details of the SEA feature:

Importance of System Health Monitoring

Keeping a regular check of health of a system is essential. To provide high-availability for a router without any downtime it is imperative to analyze the stability of a system. The stability of a system is determined by system log messages and debug traces. If any of the log messages are ignored for a significant time, it can bring a system down. Essentially, the system log messages help in analyzing the root cause of the generated event. To prevent downtime, the root cause of the problem can be identified and resolved.

Limitations of Existing Logging Mechanisms

The primary method of discovering the cause of system failure is system messages. When system messages do not provide the information needed to determine the cause of a failure, you can enable debug traces and attempt to recreate the failure. However, there are several situations in which neither of the above methods provides an optimum solution. Following are the limitations of the existing logging mechanism:

- Reviewing a large number of system messages can be an inefficient method of determining the cause of a failure.
- Debug trace is usually not configured by default.
- You cannot recreate the failure while using debug trace.
- Using debug trace is not an option if the switch on which the failure has occurred is part of your critical network.
- The problem is not reproducible when debug trace is enabled due to change in timings.
- If the system is part of a critical network, it is not advisable to recreate or debug the issue.
- Unless the problem is reproduced, the exact root cause of the system failure is not known.

Understanding the System Event Archive

The SEA feature addresses the shortcomings of the existing logging mechanism. The SEA feature can help debug issues without reproducing the problem. The SEA runs on the route processor (RP). SEA allows each CPU to report major and abnormal events to the RP using the out-of-band interface and log it into the non-volatile storage using the time-stamp. The RP logs its own events to the boot flash disk. The RP receives event messages from the cable line card and jacket card over IPC, and logs them to the boot flash.

Logging Location

By default, the SEA feature is enabled and events are stored in the log file ‘sea_log.dat’ with the timestamp. The events are stored in sea_log.dat along with the timestamp. The SEA feature requires either PCMCIA ATA Flash or Compact Flash disk for storage. By default, on PRE2 the SEA creates the log file on disk0:. The SEA command enables changing the location (disk) of the sea_log.dat file using the **logging system disk** *name* command. The size of the sea_log.dat file is 32 MB or 10% of the disk size or at least 448KB. The sea_log.dat file stores the most recent event messages in the log file in a circular fashion.

Note SEA feature does not automatically search for a disk if the default disk or explicitly configured disk is not inserted.

Managing SEA

This section describes how to manage the system event archive. The following SEA commands are used to manage the SEA functionality.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**logging system** **Example:** `Router(config)# logging system`	Enables the SEA logging feature. By default, the SEA feature is enabled. **Note** To disable the SEA logging feature, use the **no logging system** command.
Step 2	**logging system disk disk1:** **Example:** `Router(config)# logging system disk disk1:`	Changes the disk location on PRE2 or PRE4 for storing the SEA log messages. **Note** By default, SEA log messages are stored on disk0: for PRE2 and on boot flash: for PRE4.
Step 3	**show logging system** **Example:** `Router# show logging system`	Displays the latest SEA log messages stored in the sea_log.dat file.
Step 4	**show logging system disk** **Example:** `Router# show logging system disk`	Displays the disk used to store the sea_log.dat file.
Step 5	**copy logging system target** *filename* **Example:** `Router# copy logging system target filename`	Copies the sea_log.dat file to the destination file system.
Step 6	**clear logging system** **Example:** `Router# clear logging system`	Clears the events stored in the sea_log.dat file.
Step 7	**logging cmts sea** **Example:** `Router#config t`	Enables logging of system log messages to SEA.

	Command or Action	Purpose
	Example: `Router(config)# logging cmts sea`	
Step 8	**logging cmts sea syslog-level warnings** **Example:** `Router# config t` **Example:** `Router(config)# logging cmts sea syslog-level warning`	Configures the level of system log messages inclusive of and above the configured level to be stored in sea_log.dat file. The example shows the configuration to store system log messages with severity 'warning' and above to be stored in the sea_log.dat file.

Probable Scenarios and Useful SEA Commands

The table discusses the various scenarios and how to use the SEA commands for managing the event logs.

Table 220: Possible Scenarios and Useful SEA Commands

Possible Scenarios	Command Used	Explanation
To check whether SEA feature is enabled.	`Router# dir disk0:` `23 -rw-  6710888 May 16 2009 06:03:36 +00:00 sea_log.dat`	By default, SEA is enabled and the command is not shown under the "show running. To check the log file location, execute the **dir [diskname]** command from EXEC command mode. **Note** On PRE2, the default location to store the SEA log message is disk0:.
To check the latest SEA log messages.	`Router# show logging system`	To check the latest SEA log messages, execute the **show logging system** command from EXEC mode. The SEA log messages are stored with the actual time-stamp, slot/sub-slot number, name of software generating the system event, and the event message. **Tip** The sea_log.dat file is created as soon as the first SEA log message is stored in the file.
To check the current location to store the sea_log.dat file.	`Router# show logging system disk` `SEA log disk: disk0:`	If you are unsure of the disk currently storing the SEA event log messages, execute the **show logging system disk** command. As shown in the example, it displays the SEA log disk currently used to store the sea_log.dat file.
To check the last 'n' number of SEA event log messages.	`Router# show logging system last 5`	The system administrator can also check the desired number of last messages stored in the sea_log.dat file. Use the **show logging system last** *5* command to view the last 5 messages stored in the log file. **Tip** The valid range to display the last number of SEA messages is 1 to 10,000.
To change the location of the sea_log.dat file to a different disk.	`Router(config)# logging system disk disk1:` `You are configuring a different disk from the current log disk.`	To change the location of the sea_log.dat file execute the command **logging system disk diskname** from global configuration mode. **Note** After changing the disk, the new event log information is logged to the new location (in this example disk1:) and the log event information before the change disk is available at the old location (in this case disk0:).

Possible Scenarios	Command Used	Explanation
Copying the SEA event log messages to a target file.	`Router# copy logging system rcp` `Address or name of remote host []?` `192.0.2.1` `Destination username [Router]?` `username1` `Destination filename [sea_log.dat]?` `/auto/tftpboot-users/username1/sea_log.dat` `!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`	The advantage of SEA feature is that you can copy and back up SEA event log messages at specific target file locations. Use the **copy logging system target** *filename* command to copy the sea contents to the desired location. **Note** Copying the SEA event log file is useful when there is less disk space available on the disk or the disk is almost full.
To clear the SEA event log messages stored on the disk.	`Router# clear logging system` `Clear logging system operation will take a while.` `Do you want to continue? [no]: yes`	After taking a back up of SEA event log messages, you can clear the event log details stored at the default location using the **clear logging system** command. **Note** Before clearing the event log messages, it is recommended to take a back up of the SEA event log messages to a target file system.
Configuring a different disk to store the sea_log.dat file without the disk being present, provides an error message.	`Router(config)# logging system disk disk1:` `disk1: does not exist in the system`	Before changing the location of the disk, check if the target disk is present on PRE2 or PRE4. If the disk is not present then the **logging system disk disk1:** command, generates an error message. **Note** SEA will not automatically search for the disk, if the default disk is not inserted.
Configuring bootflash: as the disk to store log messages on PRE2, provides an error message.	`Router(config)# logging system disk bootflash:` `bootflash: is not allowed`	The supported disk to store the sea_log.dat file is either PCMCIA ATA flash disk or Compact Flash disk in PCMCIA jacket. If bootflash: is configured to store the log messages on PRE2 using the logging system disk bootflash: command, it generates an error message. In the example, a linear flash disk is configured to store the SEA log messages, hence an error message is shown. **Note** The SEA event log messages cannot be stored on a linear flash disk.
Changing the level of system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.	`Router(config)# logging cmts sea syslog-level warning`	

Possible Scenarios	Command Used	Explanation
		By default, the system log event message to be stored in the log file is enabled with the severity-level of system log messages being set to 'errors'. Use the **logging cmts sea syslog-level warning** command to configure the system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.

Additional References

For additional information related to health monitoring, see the following references:

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Generic Online Diagnostics (GOLD)	GOLD feature for the Cisco UBR10012 Universal Broadband Router

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

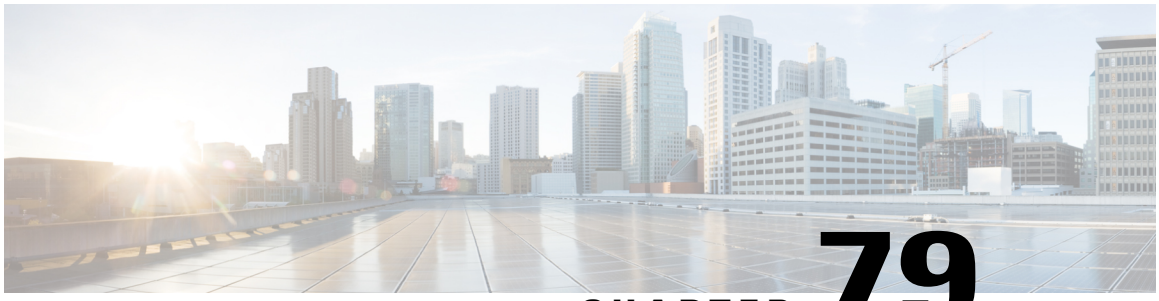
Feature Information for SEA for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 221: Feature Information for System Event Archive (SEA) for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
System Event Archive (SEA) Support for the Cisco CMTS Routers	12.2(33)SCC	The System Event Archive (SEA) is a health monitoring feature that maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. This feature was introduced for the PRE2 and PRE4 route processors. The following commands are new or modified: • **logging system** • **show logging system** • **copy logging system** • **clear logging system** • **logging cmts sea** [**syslog-level** [**level**]]



CHAPTER 79

Usage-Based Billing for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: May 10, 2010

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Usage-based Billing feature for the Cisco Cable Modem Termination System (CMTS) routers, which 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

- Feature Information for Usage-Based Billing for the Cisco CMTS Routers, page 1974

Prerequisites for Usage-based Billing

The usage-based billing feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and Cisco IOS Release 12.2SC.

Table 222: Usage-based Billing Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCA and later releases • PRE-2 Cisco IOS Release 12.2(33)SCB and later releases • PRE-4	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR-MC20X20V
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • NPE-G2 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[162]

CMTS Platform	Processor Engine	Cable Line Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

162 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

The Usage-based Billing feature has the following prerequisites:

- Cable modems must be compliant with DOCSIS 1.0 or DOCSIS 2.0 in Cisco IOS Release 12.2(33)SCA, OSSI version 3.0 in Cisco IOS Release 12.2(33)SCB and DOCSIS 3.0 in Cisco IOS Release 12.2(33)SCC and later releases.
- The Cisco CMTS router must be running Cisco IOS Release 12.2(33)SCA or later releases.
- Cable modems that are being monitored should use a DOCSIS configuration file that defines upstream and downstream primary service flows using Service Class Naming (SCN [TLV 24/25, subTLV 4]). If dynamically-created service flows are to be monitored, they should also be created with SCN names.
- When the feature is operating in File mode, an external billing server must log into the Cisco CMTS to copy the billing records to the external server, using either Secure Copy (SCP) or Trivial File Transfer Protocol (TFTP). The Cisco CMTS cannot operate as a FTP or secure FTP (SFTP) server.
- When the feature is operating in Streaming mode in non-secure mode, an external billing server must be configured to receive the billing records at a configurable TCP port.
- When the feature is operating in Streaming mode in secure mode, the following are required:
  - The external billing server must be configured to receive the billing records at a configurable TCP port using a secure socket layer (SSL) connection.

Tip Several third-party solutions for SSL support on the billing application server are available http://www.openssl.org/index.html .

- ◦ A Certificate Authority (CA) must be configured and available to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

- To use the **full-records** keyword, the Cisco CMTS router must be running the Cisco IOS Release SCC4, Cisco IOS Release SCD2, or later releases.
- To use the **flow-aggregate** keyword for ipdr/ipdr-d3 the Cisco CMTS router must be running the Cisco IOS Release SCC4, Cisco IOS Release SCD2, or later releases.

When **flow-aggregate** is enabled, the service flows are combined into one record per cable modem:

- ◦ ServiceClassName element always returns a null value in IPDR records, even when service flows on the cable modem have a valid service class name.
  ◦ ServiceIdentifier element always returns a zero value.

Restrictions for Usage-based Billing

The Usage-based Billing feature has the following restrictions and limitations:

- SNMP commands can be used to display or modify the Usage-based Billing configuration, and SNMP traps can be used to notify the billing application system when a billing record is available. However, SNMP commands cannot be used to retrieve billing records.
- Enabling IPDR mode through SNMP is not supported.
- Cisco IOS Release 12.3(9a)BC and Cisco IOS Release 12.2(33)SC do not support Usage-based Billing with 1:N or Route Processor Redundancy (RPR):
  ◦ When HCCP N+1 switchover events occur to a protect cable interface, usage-based billing is suspended until the system returns to the working cable interface.
  ◦ On the Cisco uBR10012 router, when the system switches over to the secondary PRE1 module, usage-based billing is suspended unless you have also preconfigured the usage-based billing on the secondary PRE1 module.

- The **ipdr template** command allows the user to add an IPDR template to the desired session (based on session ID) on the Cisco CMTS. Only the system-supported templates can be added. The system-supported templates list can be viewed by entering "?" at the command prompt.

The **cable sflog** command specifies the logging mechanism for deleted SNMP service flows. For those items that meet its criteria, are stored on the cable line card side (these items can be also be queried by the docsQosServiceFlowLogTable, docsQos3ServiceFlowLogTable, and docsIetfQosServiceFlowLogTable MIBs). The other items are stored on the route processor (RP) side of the sflog file.

During a line card switchover, the items in the line card side are lost. Similarly, during a PRE switchover, those items in the RP side of the sflog file are lost.

If the user uses the SAMIS file destination, a PRE switchover also reinitializes that output file

- Billing records do not include information about multicast service flows and traffic counters.

- The packet counters displayed by CLI commands are reset to zero whenever the Cisco CMTS router is rebooted. The packet counters displayed by SNMP commands are not retained across router reloads, and SNMP MIB counters cannot be preserved during reloads. These counters are 64-bit values and could roll over to zero during periods of heavy usage.
- When configuring cable metering in the usage-based billing File Mode, the source-interface cannot be specified immediately after using the cable metering filesystem command. Once the cable metering filesystem command is used, the cable metering file will write to the bootflash. Until this operation is complete, no cable metering configuration will be allowed. After the file write operation is complete, the source-interface command (cable metering source-interface) can then be configured; and the metering file in the bootflash would need to be removed so that billing packets have the source-interface's IP address.

Note This cable metering restriction will not be a problem during reload.

- When configuring cable metering in the usage-based billing Streaming Mode, make sure that the loopback interface is accessible from the collector server. Telnetting to the IP address of the loopback interface from the collector server is a good method of testing whether the loopback interface is accessible from the collector server or not.
- To use the **full-records** and **flow-aggregate** keywords, the router must be running the Cisco IOS Release SCC3, or Cisco IOS Release SCD1, or later releases.

Information About Usage-based Billing

Feature Overview

The Usage-based Billing feature provides a standards-based, open application approach to recording and retrieving traffic billing information for DOCSIS networks. When enabled, this feature provides the following billing information about the cable modems and customer premises equipment (CPE) devices that are using the cable network:

- IP and MAC addresses of the cable modem.
- Service flows being used (both upstream and downstream service flows are tracked).
- IP addresses for the CPE devices that are using the cable modem.
- Total number of octets and packets received by the cable modem (downstream) or transmitted by the cable modem (upstream) during the collection period.
- Total number of downstream packets for the cable modem that the CMTS dropped or delayed because they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA).

Billing records are maintained in a standardized text format that the service provider can easily integrate into their existing billing applications. Service providers can use this information to determine which users might be potential customers for service upgrades, as well as those customers that might be trying to exceed their SLA limits on a regular basis.

Usage-Based Billing and DOCSIS Support on the Cisco CMTS Routers

The usage-based billing feature supports these DOCSIS features on the Cisco CMTS routers:

- DOCSIS 1.0, DOCSIS 2.0, and DOCSIS 3.0 compliant cable modems are supported.
- Best Effort service flows are supported for DOCSIS-compliant cable modems.
- Secondary service flows are supported for DOCSIS-compliant cable modems.
- Dynamic service flows are supported for DOCSIS-compliant cable modems.
- Information about deleted service flows is available only for DOCSIS 1.1 service flows but not for DOCSIS 1.0 service flows.
- Support for terminated service flows must be enabled using the **cable sflog** command in global mode.

Standards

The Usage-based Billing feature is based on several open standards, allowing it to be supported by a wide range of commercial and custom-written billing applications. The following standards provide the major guidelines for writing and using the billing records that the CMTS produces:

- Extensible Markup Language (XML)—A metalanguage that in turn can easily define other markup languages to contain any kind of structured information, such as billing records. An XML-based approach allows the collected billing information to be used by and distributed among many different billing applications from different vendors. It also allows the format to be easily updated and customized to meet the needs of different providers.
- IP Detail Record (IPDR)—An open, vendor-independent standard, defined in the *Network Data Management—Usage (NDM-U) For IP-Based Services* specification, to simplify billing and usage record-keeping for any type of services that can be delivered over an IP-based network. Service providers can use IPDR to create unified billing applications for all of their services, such as DOCSIS or Voice-over-IP, even though those services use different protocols and application servers.
- DOCSIS Operations Support System Interface (OSSI) specification—A DOCSIS specification that defines the requirements for the network management of a DOCSIS network, including a Subscriber Account Management Interface Specification (SAMIS) for a billing record interface. The DOCSIS 2.0 version of this specification states that a CMTS is not required to provide a billing interface, but if the CMTS does provide a billing interface, it must be based on the IPDR/XML standards.

Tip For further information about these standards, see the documents listed in the “Standards” section on page 38 .

IPDR Service Definition Schemas

To standardize the management of objects, service definition schemas are associated with IPDR just as MIBs are associated to SNMP.

For more information, see the OSSI specification document at http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-OSSIv3.0-I02-070223.pdf

The schemas are supported on Cisco IOS Release 12.2(33)SCC4, 12.2(33)SCD2, and later releases.

Table 223: IPDR Schema List for DOCSIS 3.0

Category	Service Definition	Schema Definition	Collection Method
SAMIS	SAMIS-TYPE-1	DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd	time interval, ad-hoc
	SAMIS-TYPE-2	DOCSIS-SAMIS-TYPE-2_3.5.1-A.1.xsd	time interval, ad-hoc
Diagnostic Log Service Definition Schemas	DIAG-LOG-TYPE	DOCSIS-DIAG-LOG-TYPE_3.5.1-A.1.xsd	ad-hoc
	DIAG-LOG-EVENT-TYPE	DOCSIS-DIAG-LOG-EVENT-TYPE_3.5.1-A.1.xsd	event
	DIAG-LOG-DETAIL-TYPE	DOCSIS-DIAG-LOG-DETAIL-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
Spectrum Management	SPECTRUM-MEASUREMENT-TYPE	DOCSIS-SPECTRUM-MEASUREMENT-TYPE_3.5-A.1.xsd	time interval, ad-hoc
CMTS CM Registration Status Information	CMTS-CM-REG-STATUS-TYPE	DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
CMTS CM Upstream Status Information	CMTS-CM-US-STATS-TYPE	DOCSIS-CMTS-CM-US-STATS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc
CMTS Topology	CMTS-TOPOLOGY-TYPE	DOCSIS-CMTS-TOPOLOGY-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CPE Information	CPE-TYPE	DOCSIS-CPE-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CMTS Utilization Statistics	CMTS-US-UTIL-STATS-TYPE	DOCSIS-CMTS-US-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event
	CMTS-DS-UTIL-STATS-TYPE	DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event

The schemas listed in the table are supported by implementing the respective Collectors, which work as SNMP agents to generate these IPDR records according to management information of the system.

DOCSIS SAMIS Service Definitions

SAMIS for DOCSIS 3.0 service definitions are well structured and has two versions—SAMIS-TYPE-1 and SAMIS-TYPE-2 and provide a different level of information details than SAMIS.

DOCSIS 2.0 SAMIS supports only event session (default type) and DOCSIS 3.0 SAMIS TYPE 1 and DOCSIS 3.0 SAMIS TYPE 2 support only interval and ad-hoc sessions.

SAMIS is collected based on configurable time intervals. Each interval is a different document and the Exporter stops and starts a new session for a new interval. The interval starts from the last metering that has either succeeded or failed, unlike the time-interval session that has a fixed starting point and an interval.

Note The SAMIS schema can be configured with the **cable metering ipdr session** command SAMIS-TYPE-1 and SAMIS-TYPE-2 schemas can be configured through the **cable metering ipdr-d3** command. These schemas are mutually exclusive of each other.

Limitation To DOCSIS SAMIS

- Only a schema that is consistent with the **cable metering ipdr| ipdr-d3** command will work. If none of the schemas are consistent, none of them will work.
- Changing the SAMIS IPDR type will abort exporting IPDR data.

DOCSIS Diagnostic Log Service Definitions

This service definition defines the IPDR Streaming using a two-step process:

- SNMP or other configuration management interface, such as the CLI is used to configure the Diagnostic Log.
- IPDR/SP is used to stream the Diagnostic Log instances.

These Diagnostic Log service definition schemas support the following collection methods:

- The Cisco CMTS supports streaming of the DIAG-LOG-TYPE record collections as an ad-hoc session.
- The Cisco CMTS supports streaming of DIAG-LOG-EVENT-TYPE record collections as an event session. For event-based Diagnostic Log records, the Cisco CMTS streams the record when the event is logged in the Diagnostic Log and an IPDR message is transmitted to the Collector.
- The DOCSIS-DIAG-LOG-DETAIL-TYPE supports the following collection methods:
  - Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the diagnostic log, then streams the record to the Collector associated with this session. For time interval based Diagnostic Log records, the Cisco CMTS streams a snapshot of the Diagnostic Log at the scheduled collection time.
  - Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the diagnostic record and send the data to the Collector.
  - Event—When a diagnostic log record is created, an ipdr message is transmitted to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS Spectrum Measurement Service Definition

This service definition schema defines the IPDR schema for the enhanced signal quality monitoring feature.

The DOCSIS-SPECTRUM-MEASUREMENT-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the spectrum information, then streams the records to the Collector.

- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the spectrum information and send the data to the Collector.

DOCSIS CMTS CM Registration Status Service Definition

This service definition schema defines the IPDR service definition schema for the CMTS CM Registration Status information.

The DOCSIS-CMTS-CM-REG-STATUS-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CM status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all status information of the cable modems and send the data to the Collector.
- Event—When a cable modem goes from "offline" status to "online" or changes to "offline" from "online" (not including intermediate state changes), the Exporter invokes the application to collect the cable modem status information and sends the data to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS CM Upstream Status Service Definition

This service definition schema define the cable modem registration status objects and upstream status objects from the cable modem and the Cisco CMTS perspective. In the CmtsCmUsEqData IPDR schema field, configure the **cable upstream equalization-coefficient** command under the corresponding MAC domain to enable the feature to have data. For more information on this command, see the Cisco IOS CMTS Cable Command Reference Guide .

The DOCSIS-CMTS-CM-US-STATS-TYPE schema support the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the cable modem upstream status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all upstream status information of the cable modem and send the data to the Collector.

DOCSIS CMTS Topology Service Definition

In the case of an event session, the event means a change of the topology.

This service definition schema defines the IPDR service definition schema for the CMTS Topology information.

The DOCSIS-CMTS-TOPOLOGY-TYPE schema supports the following collection methods:

- Ad-hoc—Sends the entire picture of all fiber-nodes.
- Event—Sends only the updated channels status of the fiber nodes.

DOCSIS CPE Service Definition

The DOCSIS-CPE-TYPE schema supports the following collection methods:

- Ad-hoc—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CPE status information, then transfers the records to the Collector.
- Event—When new CPE is added, the status of the CPE changes (including change in IP address), or a new CPE replaces an old one (in this case, two messages are displaced— removal of the old CPE and addition of the new CPE). For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS Utilization Statistics Service Definition

The CMTS Utilization Statistics mainly focuses on channel utilization. It covers CMTS MAC Domain, channel identifier, and the upstream or downstream utilization attributes and counters.

The DOCSIS-CMTS-US-UTIL-STATS-TYPE schemas defines upstream utilization statistics for a specified upstream logical channel interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

The DOCSIS-CMTS-DS-UTIL-STATS-TYPE schema defines downstream utilization statistics for a specified downstream interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

For more information, see the IPDR Streaming Protocol on the Cisco CMTS Routers guide at the following URL:

IPDR Streaming Protocol

These schemas support only interval-driven event session for the entire downstream and upstream. The interval is defined in the docsIfCmtsChannelUtilizationInterval MIB and it creates document for every exporting.

Note The UsUtilTotalCntnReqDataMslots, UsUtilUsedCntnReqDataMslots, and UsUtilCollCntnReqDataMslots MIBs are not supported on the Cisco CMTS implementation.

The DsUtilTotalBytes MIB for RF Gateway RF channels is the maximum counter of bytes this RF channel can pass during an interval.

Modes of Operation

The Usage-based Billing feature can operate in three modes:

- File Mode—In file mode, the CMTS collects the billing record information and writes the billing records to a file on a local file system, using a file name that consists of the router's hostname followed by a timestamp of when the file was written. A remote application can then log into the CMTS and transfer the billing record file to an external server where the billing application can access it.

The remote application can use the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP) to transfer the file. After a successful transfer, the remote application then deletes the billing record file, which signals the CMTS that it can create a new file. The remote application can either periodically log into the CMTS to transfer the billing record file, or it can wait until the CMTS sends an SNMPv2 trap to notify the application that a billing record file is available.

- Streaming Mode—In streaming mode, the CMTS collects the billing record information and then regularly transmits the billing record file to an application on an external server, using either a non-secure

TCP connection or a secure sockets layer (SSL) connection. The billing record data collected is streamed in real time; and if streaming is unsuccessful, then the SAMIS data is sent only at the next interval.

If the CMTS fails to establish a successful connection with the external server, it retries the connection between one to three times, depending on the configuration. If the CMTS continues to fail to connect with the external server, the Cisco CMTS sends an SNMPv2 trap to notify the SNMP manager that this failure occurred.

In streaming mode, you can configure the CMTS to transmit the billing record file at regular intervals. Typically, the interval chosen would depend on the number of cable modems and the size of the billing record files that the CMTS produces.

- IPDR Mode—In the IPDR mode, the IPDR export process communicates with IPDR Collectors. The architecture supports multiple Collectors distinguished by priority value for failover purposes. The smaller the number of Collectors, the higher is the priority value. Associating one session to two or more Collectors with the same priority value is regarded as random priority. At any given time, data is sent to only the available highest priority Collector. If the highest priority Collector connection fails due to any reason, the data is sent to the next available highest priority Collector. After a higher priority Collector comes back online, it will fail over again. Depending on the network configuration, you can have different primary Collectors for different IPDR sessions. For example, there may be a billing Collector or a diagnostic Collector.

Billing Record Format

Each billing record is an ASCII text file using XML formatting to encode the billing record objects that are required by the DOCSIS specifications. This file can be read by any billing application that can be configured to parse XML data files.

The table lists the objects that are contained in each billing record that the CMTS generates. This table shows the object's name, as it appears in the billing record, and a description of that object.

Table 224: Billing Record Objects

Object Name	Description
IPDRcreationTime	(Appears in header of billing record) Date and time that the CMTS created the billing created. Cisco uBR10012 router provides UTC timestamps for IPDR timestamping feature. To provide usage records with local time timestamping, use the **cable metering localtime** command. The IPDRcreationTime field in the Billing records shows the localtime timestamp as the time of creation of the record when it is enabled using the **cable metering localtime** command. If the localtime timestamping is not enabled, then the default UTC timestamp (indicated by a Z after the timestamp) is shown as time of creation of the record. For example, when the local time timestamping is enabled, the timestamp in metering output is local time "2015-03-03T16:26:07", otherwise the timestamp is the UTC time "2015-03-03T16:26:07Z" (with a "Z" indicating that the time is UTC).)

Object Name	Description
serviceClassName	Service Class Name (SCN) identifying the service flow (for example, BronzeDS). **Note** Cisco IOS Release 12.3(9a) and Cisco IOS Release 12.2(33)SC support DOCSIS 1.0 and DOCSIS 1.1 cable modems with the following differences between them: • Because DOCSIS 1.0 cable modems do not have service class names, the SCN field is always blank and the service flow ID (SFID) is the same as the service ID (SID). • For DOCSIS 1.1 cable modems, the value for the SCN field is what is configured and the SFID.
CMmacAddress	MAC Address of the cable modem, expressed as six hexadecimal bytes separated by dashes (for example, 00-00-0C-01-02-03).
CMipAddress	IP address for the cable modem, expressed in dotted decimal notation (for example, 192.168.100.101).
CMdocsisMode	Version of DOCSIS QoS provision that the cable modem is currently using (DOCSIS 1.0 or 1.1).
CPEipAddress	IP address for each CPE device that is using this cable modem, expressed in dotted decimal notation. This object is optional and can be suppressed to improve performance by reducing the size of the billing record files.
CMTSipAddress	IP address for the CMTS, expressed in dotted decimal notation.
CMTShostName	Fully qualified hostname for the CMTS (for example, cmts01.cisco.com).
CMTSsysUpTime	Amount of time, in hundredths of a second, since the last initialization of the CMTS management interface, expressed as a 32-bit decimal number (0 to 4,294,967,296).

Object Name	Description
RecType (SFType renamed to RecType in Cisco IOS Release 12.3(17a)BC)	Type of service flow being described: • **Interim—**the service flow was active throughout the collection period and should be reported as 1. • **Stop—**the service flow was deleted at some point during the collection period and should be reported as 2.
serviceIdentifier	Service flow ID assigned to this service flow by the CMTS, expressed as a decimal number. **Note** For DOCSIS 1.0 cable modems, the SFID field always shows the primary service flow for the upstream or downstream.
serviceDirection	Direction for the service flow (**Downstream** or **Upstream**).
serviceOctetsPassed	Total number of octets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
servicePktsPassed	Total number of packets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
SLAdropPkts	(Downstream service flows only) Total number of downstream packets for the cable modem that the CMTS dropped because otherwise they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
SLAdelayPkts	(Downstream service flows only) Total number of packets that the CMTS delayed transmitting on the downstream to the cable modem because otherwise they would have exceeded bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
CMTScatvIfIndex	The ifIndex of the MAC interface.
CMTScatvIfName	The ifName of the CMTS CATV (MAC) interface associated with this cable modem.

Object Name	Description
CMTSupIfName	The ifName of the CMTS Upstream interface associated with this cable modem.
CMTSdownIfName	The ifName of the CMTS Downstream interface associated with this cable modem.
CMcpeFqdn	FQDNs for cable modem associated CPEs.
serviceTimeCreated	Timestamp for SF creation (consistent with QoS MIB model).
serviceTimeActive	The active time of the SF in seconds.

Note Because the byte and packet counters are 64-bit values, it is possible for them to wrap around to zero during a billing period. The billing application should use the sysUpTime value along with the counters to determine whether the counters have wrapped since the last billing period. If a counter appears to regress, and if the current sysUpTime indicates this billing cycle is the next scheduled cycle for this particular cable modem, you can assume that the counter has wrapped during the billing cycle.

Note These billing record objects are defined in Appendix B, *IPDR Standards Submission for Cable Data Systems Subscriber Usage Billing Records* , in the *DOCSIS 2.0 OSSI Specification* (SP-OSSIv2.0-IO3-021218).

The following example shows a sample IPDR billing record for a downstream service flow:

```
<?xml version="1.0" encoding="UTF-8"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="C341A679-0000-0000-0000-000BBF54D000"
creationTime="2002-05-25T14:41:29Z"
IPDRRecorderInfo="CMTS01"
version="3.1">
</IPDR>
<IPDR xsi:type="DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-AB-D4-53</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.3</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>2</serviceDirection>
<serviceOctetsPassed>23457</ServiceOctetsPassed>
```

```
<servicePktsPassed>223</ServicePktsPassed>
<serviceSlaDropPkts>2</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

The following example shows a sample IPDR billing record for an upstream service flow:

<?xml version="1.0" encoding="UTF-8"?>

```
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="docId="C3146152-0000-0000-0000-000BBF7D5800"
creationTime="2003-09-18T16:52:34Z"
IPDRRecorderInfo="CMTS01-UBR7246.cisco.com"
version="3.1">
<IPDR xsi:type=" DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-18-8A-4D</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.14</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>1</serviceDirection>
<serviceOctetsPassed>1404</ServiceOctetsPassed>
<servicePktsPassed>6</ServicePktsPassed>
<serviceSlaDropPkts>0</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

SNMP Support

Cisco IOS Release 12.3(9a)BC and Cisco IOS Release 12.2(33)SC support the following MIBs that provide SNMPv2 support for the Usage-based Billing feature:

CISCO-CABLE-METERING-MIB

- Supports configuration of the usage-based billing feature using SNMPv2 commands.
- Displays the current usage-based billing configuration using SNMPv2 commands.
- Sends SNMPv2 traps based on the following usage-based billing events:
  - The Cisco CMTS reports that a new billing record is available.
  - The Cisco CMTS reports that a failure occurred in writing the most recent billing record (for example, the disk is full).
  - The Cisco CMTS reports that it could not successfully open a secure SSL connection to stream a billing record to the billing server.

CISCO-CABLE-WIDEBAND-MIB
Sets the polling interval for calculating the utilization of an RF channel by using the **ccwbRFChanUtilInterval** object.

DOCS-QOS-MIB

- Sets the load and utilization of both upstream and downstream physical channels through the **docsIfCmtsChannelUtilizationInterval** object. This information may be used for capacity planning and incident analysis, and may be particularly helpful in provisioning high value QoS.
- Displays information about all service flows (DOCSIS 1.1 service flows only) including multicast service flow is maintained in the **docsQosServiceFlowLogTable** in DOCS-QOS-MIB, **docsIetfQosServiceFlowLogTable** in DOCS-IETF-QOS-MIB, and **docsQos3ServiceFlowLogTable** in DOCS-QOS3-MIB.

To view information about deleted service flows, enable logging of deleted service flows using the **cable sflog** global configuration command.

Benefits

The usage-based billing feature provides the following benefits to cable service providers and their partners and customers:

- Allows service providers to integrate their billing applications for DOCSIS services with their other XML-capable billing applications.
- Standards-based approach that supports existing networks and services, such as DOCSIS and PacketCable, and is easily extensible to support future services as they are supported on the Cisco CMTS.

How to Configure the Usage-based Billing Feature

This section describes the following tasks that are required to implement the Usage-based Billing feature:

Enabling Usage-based Billing Feature File Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router#`	
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**cable metering filesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**] **Example:** `Router(config)# cable metering filesystem harddisk:` **Example:** `Router(config)#`	Enables the Usage-based Billing feature for file mode and configures it. The system will write the billing records on this file system using a file name that contains the hostname of the router followed by a timestamp when the record was written.
Step 4	**snmp-server enable traps cable metering** **Example:** `Router(config)# snmp-server enable traps cable metering` **Example:** `Router(config)#`	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.
Step 5	**cable sflog max-entry** *number* **entry-duration** *time* **Example:** `Router(config)# cable sflog max-entry 2000 entry-duration 7200` **Example:** `Router(config)#`	(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.
Step 6	**cable metering source-interface** *interface* **Example:** `Router(config)# cable metering source-interface loopback100`	(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 7	**end** **Example:** `Router(config)# end` **Example:** `Router#`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature File Mode Using SNMP Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

To configure the Cisco CMTS for Usage-based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command.

Table 225: SNMP Objects to be Configured for File Mode

Object	Type	Description
ccmtrCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.

Object	Type	Description
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).

Object	Type	Description
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmtrCollectionType object to 2, to enable the Usage-based Billing feature and to configure it for file mode:

Example:

```
workstation# setany -v2c

ip-address rw-community-string

ccmtrCollectionType.0 -i 2

workstation#
```

Step 2 Set the ccmtrCollectionFilesystem object to the local file system where the Cisco CMTS should write the billing records:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

Step 3 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmtrCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

Step 4 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmtrCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
```

```
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

Step 5 (Optional) To specify the source-interface for the billing packets, set the ccmtrtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for Enabling Usage Billing using SNMP Mode

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = none(1)
ccmtrCollectionFilesystem.0 =
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = 0
ccmtrCollectionDestination.0 =
ccmtrCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for file mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionType.0 -i 2
workstation# setany -v2c 10.8.8.21 rw-string
ccmtrCollectionFilesystem
.0 -D disk1:
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering filesystem disk1:
Router#
```

The following SNMP display shows the new configuration, after the Cisco CMTS has successfully written a billing record:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = local(2)
ccmtrCollectionFilesystem.0 = disk1:
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = success(1)
ccmtrCollectionDestination.0 = disk1:UBR7246.cisco.com-20030925-185827
```

```
ccmtrCollectionTimestamp.0 = 07 d3  09 19   12 3a  1c 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling Usage-based Billing Feature Streaming Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**cable metering destination** *ip-address port* [*ip-address2 port2*] *retries minutes* {**non-secure** | **secure**} [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**] **Example:** `Router(config)# cable metering destination 10.10.21.3 5300 10.10.21.4 5300 2 30 secure` **Example:** `Router(config)#`	Enables the Usage-based Billing feature for streaming mode and configures it with the following parameters:
Step 4	**snmp-server enable traps cable metering** **Example:** `Router(config)# snmp-server enable traps cable metering`	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 5	**cable sflog max-entry** *number* **entry-duration** *time* **Example:** `Router(config)# cable sflog max-entry 2000 entry-duration 7200` **Example:** `Router(config)#`	(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.
Step 6	**cable metering source-interface** *interface* **Example:** `Router(config)# cable metering source-interface loopback100` **Example:** `Router(config)#`	(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.
Step 7	**end** **Example:** `Router(config)# end` **Example:** `Router#`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature Streaming Mode Using SNMP Commands

This section describes how to use SNMP commands to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

To configure the Cisco CMTS for Usage-based Billing feature in streaming mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

Note In addition, to include information about deleted service flows (DOCSIS 1.1 service flows only) in the billing records, you must enable the logging of deleted service flows, using the **cable sflog** global configuration command. See the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

Cisco CMTS Cable Command Reference

Table 226: SNMP Objects to be Configured for Streaming Mode

Object	Type	Description
cdxCmtsMode	Integer	

Object	Type	Description
		Enables or disables the Usage-based Billing feature. The valid values are: • true—Enables the Usage-based Billing feature. This is the default value. • false—Disables the Usage-based Billing feature. This is the default value. • start-stop—Enables the Usage-based Billing feature. This is the default value. Set docsQosCmtsBaseEntry to 3

Object	Type	Description
		(system) to enable the feature for streaming mode.
cdxCollectorIpAddress	InetAddress	IP address for the external collection server. This value must be specified

Object	Type	Description
ccmCollectionPort	Unsigned32	TCP port number at the external collection server to which the billing records should be sent. The valid range is 0 to 65535, but you should not specify a port in the well-known range of 0 to 1024. This value must be specified

Note You can configure the ccmCollectionIpAddress and ccmCollectionPort objects twice, to specify a primary collection server and a secondary collection server.

Object	Type	Description
[illegible]	[illegible]	(Optional) Type of IP address being used for the collection server. The only valid value is ipv4, which is the default value.

Object	Type	Description
[illegible]	Unsigned32	(Optional) Specifies how often, in minutes, the billing records are transmitted to the external server. The valid range is 2 to 1440 minutes (24 hours), with a default of 30 minutes. (We recommend a minimum interval of 30 minutes)

Object	Type	Description
[illegible]	Unsigned32	(Optional) Specifies the number of retry attempts that the CMTS will make to establish a secure connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range for *n* is 0 to 5, with a default of 0.

Object	Type	Description

Note The ccmCollectionInterval and ccmCollectionRetries parameters are optional when configuring usage-based billing for streaming mode with SNMP commands, but these parameters are required when configuring the feature with CLI commands.

Object	Type	Description
[illegible]	[illegible]	

Object	Type	Description
		(Optional) Specifies whether the Cisco CMTS should use a secure socket layer (SSL) connection when connecting with the billing application on the external server. The valid values are: • [illegible]

Object	Type	Description

Object	Type	Description
[illegible]	[illegible]	

Object	Type	Description
		(Optional) Indicates whether IP address for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • false—Specifies that IP addresses for CPE devices are included in the billing records. • true—Specifies that IP addresses for CPE devices are omitted from the billing records. **Note** When set to

Object	Type	Description
		true, a maximum of 5 CPE IP addresses for each cable modem.

Object	Type	Description
[illegible]	[illegible]	

Object	Type	Description
		(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • [illegible]

Object	Type	Description

Object	Type	Description
		(Optional) Specifies the source for the billing packets

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmCollectionType object to 3, to enable the Usage-based Billing feature and to configure it for streaming mode:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionType.0 -i 3
workstation#
```

Step 2 Set the ccmCollectionIpAddress and ccmCollectionPort objects to the IP address of the external collection server and the TCP port number to which billing records should be sent:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 6789

workstation#
```

Step 3 (Optional) Set the ccmCollectionIpAddress and ccmCollectionPort objects a second time to specify the IP address and TCP port number of a second external collection server to which billing records should be sent, in the case that the Cisco CMTS cannot connect to the primary collection server:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0c'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 7000

workstation#
```

Step 4 (Optional) To change any of the other default parameters, set the appropriate objects to the desired values. For example, the following lines configure the Usage-based Billing feature for a non-secure connection, with a collection interval of 45 minutes, and a maximum number of 3 retries.

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionSecure.1 -i 2
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionInterval.1 -i 45
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionRetries.1 -i 3
workstation#
```

Step 5 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c
```

```
ip-address rw-community-string
 ccmCollectionCpeList.0 -i 2
workstation#
```

Step 6 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmCollectionAggregate.0 -i 1
workstation#
```

Step 7 (Optional) To specify the source-interface for the billing packets, set the ccmtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for SNMP Commands

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = none(1)
ccmCollectionFilesystem.0 =
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for streaming mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionType.0 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionPort.1 -g 6789

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionRetries.1 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionInterval.1 -i 45
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering destination 10.8.6.11 6789 3 45 non-secure
Router#
```

The following SNMP display shows the new configuration:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = stream(3)
ccmCollectionFilesystem.0 =
ccmCollectionIpAddrType.1 = ipv4(1)
ccmCollectionIpAddress.1 = 0a 08  06 0b
ccmCollectionPort.1 = 6789
ccmCollectionInterval.1 = 45
ccmCollectionRetries.1 = 3
ccmCollectionSecure.1 = false(2)
ccmCollectionRowStatus.1 = active(1)
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling Usage-based Billing Feature File Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable metering filesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**] **Example:** `Router(config)# cable metering filesystem harddisk:` **Example:** `Router(config)#`	Enables the Usage-based Billing feature for file mode and configures it. The system will write the billing records on this file system using a file name that contains the hostname of the router followed by a timestamp when the record was written.
Step 4	**snmp-server enable traps cable metering** **Example:** `Router(config)# snmp-server enable traps cable metering` **Example:** `Router(config)#`	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.
Step 5	**cable sflog max-entry** *number* **entry-duration** *time* **Example:** `Router(config)# cable sflog max-entry 2000 entry-duration 7200` **Example:** `Router(config)#`	(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.
Step 6	**cable metering source-interface** *interface* **Example:** `Router(config)# cable metering source-interface loopback100` **Example:** `Router(config)#`	(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.
Step 7	**end** **Example:** `Router(config)# end` **Example:** `Router#`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature File Mode Using SNMP Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

To configure the Cisco CMTS for Usage-based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command.

Table 227: SNMP Objects to be Configured for File Mode

Object	Type	Description
ccmtrCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.

Object	Type	Description
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmtrCollectionType object to 2, to enable the Usage-based Billing feature and to configure it for file mode:

Example:

```
workstation# setany -v2c

ip-address rw-community-string

ccmtrCollectionType.0 -i 2

workstation#
```

Step 2 Set the ccmtrCollectionFilesystem object to the local file system where the Cisco CMTS should write the billing records:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

Step 3 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmtrCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

Step 4 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmtrCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

Step 5 (Optional) To specify the source-interface for the billing packets, set the ccmtrtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
```

```
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Enabling and Configuring the Secure Copy Protocol (optional)

This section describes how to configure the Cisco CMTS for the Secure Copy Protocol (SCP), which allow an external server to log in to the Cisco CMTS and copy the billing records from the Cisco CMTS to the external server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable` **Example:** `Router#`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model` **Example:** `Router(config)#`	Enables the Authentication, Authorization, and Accounting (AAA) access control model.
Step 4	**aaa authentication login** {**default** | *list-name* } *method1* [*method2* ...] **Example:** `Router(config)# aaa authentication login default enable`	Enables AAA access control authentication at login, using the following parameters: Valid methods include **enable**, **line**, and **local**.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 5	**aaa authorization exec** {**default** | *list-name* } *method1* [*method2* ...] **Example:** `Router(config)# aaa authorization exec default local` **Example:** `Router(config)#`	Configures the CMTS to allow users to run an EXEC shell and access the CLI to run the Secure Copy commands. Valid methods include **local**.
Step 6	**username** *name* **privilege** *level* **password** *encryption-type password* **Example:** `Router(config)# username billingapp privilege 15 password 7 billing-password` **Example:** `Router(config)#`	(Optional) Creates a user account for login access and specifies the privilege level and password for that account: **Note** This step is optional but for the purposes of security and management, Cisco recommends creating a unique account for the billing application to use when logging into the CMTS.
Step 7	**ip ssh time-out** *seconds* **Example:** `Router(config)# ip ssh time-out 120` **Example:** `Router(config)#`	Enables Secure Shell (SSH) access on the Cisco CMTS, which is required for SCP use. The *seconds* parameter specifies the maximum time allowed for SSH authentication, in seconds, with a valid range of 0 to 120 seconds, with a default of 120 seconds.
Step 8	**ip ssh authentication-retries** *n* **Example:** `Router(config)# ip ssh authentication-retries 3` **Example:** `Router(config)#`	Specifies the maximum number of login attempts a user is allowed before the router disconnects the SSH session. The valid range is 1 to 5, with a default of 3 attempts.
Step 9	**ip scp server enable** **Example:** `Router(config)# ip scp server enable`	Enables SCP access on the Cisco CMTS.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 10	**end** **Example:** `Router(config)# end` `Router#`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Cisco CMTS for SSL Operation

This section describes the procedures to configure the Cisco CMTS for secure socket layer (SSL) operation, so that the Usage-based Billing feature can use an SSL connection to transfer the billing record files in streaming mode.

Note This procedure is required only when using the **secure** option with the **cable metering destination** command.

Prerequisites for CA

- The billing application server must be configured for SSL operations.
- A Certificate Authority (CA) must be configured to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

SUMMARY STEPS

To prepare the Cisco CMTS router for SSL operation, you must perform the following configuration steps:

- Configuring the router's host name and IP domain name, if not already done.
- Generating an RSA key pair.
- Declaring a Certification Authority.
- Configuring a Root CA (Trusted Root).
- Authenticating the CA.
- Requesting the Certificates.

For the detailed steps in performing these procedures, see the Configuring Certification Authority Interoperability

Retrieving Records from a Cisco CMTS in File Mode

When the Usage-based Billing feature is enabled and configured for File mode, the billing application server must regularly retrieve the billing records from the Cisco CMTS. This is typically done by a script that either logs in to the Cisco CMTS and uses CLI commands to transfer the file, or by a script that uses SNMP commands to transfer the file.

When using CLI commands, the procedure is typically as follows:

1. The billing application server receives an SNMP trap from the Cisco CMTS when a billing record is written. This notification contains the file name of the billing record that should be retrieved.
2. The billing application server starts a custom-written script to retrieve the billing record. This script would do one of the following:
   a. If using CLI commands, the script logs in to the Cisco CMTS using a telnet connection, and then transfers the billing record to the billing application server, using the **copy** CLI command. The transfer can be done using either the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP).

Note You could also use the File Transfer Protocol (FTP) to transfer files from the Cisco CMTS to an external FTP server, but this is not recommended, because the FTP protocol transmits the login username and password in cleartext.

1. If using SNMP commands, the script sets the ciscoFlashCopyEntry objects in the CISCO-FLASH-MIB to transfer the billing record to the application server, using TFTP.
2. After transferring the billing record, the script deletes it on the Cisco CMTS file system, so that the Cisco CMTS can begin writing a new billing record.

The following sections show examples of how this can be done, using each method.

Tip The following examples are given for illustration only. Typically, these commands would be incorporated in automated scripts that would retrieve the billing records.

Using SCP

To transfer billing records using SCP, you must first enable and configure the router for SCP operation, using the procedure given in the “Enabling and Configuring Secure Copy (optional)” section on page 21 . Then, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the SCP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an FTP server with the hostname of billserver.mso-example.com:

```
CMTS01# copy slot0:CMTS01_20030211-155025 scp://billingapp-server.mso-example.com/

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
Password: billing-password
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1403352/1024 bytes]
1403352 bytes copied in 17.204 secs (85631 bytes/sec)
CMTS01# delete slot0:CMTS01_20030211-155025

CMTS01# squeeze slot0:

CMTS01#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using TFTP

To transfer billing records using TFTP, you must first configure an external workstation to be a TFTP server. For security, the TFTP server should be isolated from the Internet or any external networks, so that only authorized TFTP clients, such as the Cisco CMTS router, can access the server.

To transfer the billing records, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the TFTP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an TFTP server with the hostname of billserver.mso-example.com.

```
Router# copy slot0:CMTS01_20030211-155025 tftp://billingapp-server.mso-example.com/incoming

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1102348/1024 bytes]
1102348 bytes copied in 14.716 secs (63631 bytes/sec)
Router# delete slot0:CMTS01_20030211-155025

Router# squeeze slot0:

Router#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using SNMP

To transfer billing record file using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB to transfer the file to a TFTP server. After the file has been successfully transferred, you can then use SNMp commands to delete the billing record file.

Note Before proceeding with these steps, ensure that the TFTP server is properly configured to receive to receive the billing records. At the very least, this means creating a directory that is readable and writable by all users. On some servers, the TFTP server software also requires that you create a file with the same name as the file that is to be received, and this file should also be readable and writable by all users.

To transfer a billing record file to a TFTP server, using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB.

Table 228: Transferring a File to a TFTP Server Using SNMP Commands

Object	Type	Description
ciscoFlashCopyEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashCopyCommand	INTEGER	Type of copy command to be performed. To copy a billing record file to a TFTP server, set this object to 3 (copyFromFlash).
ciscoFlashCopyServerAddress	IpAddress	IP address of the TFTP server. **Note** This parameter defaults to the broadcast address of 255.255.255.255, which means it will transfer the billing record file to the first TFTP server that responds. For security, this object should always be set to the IP address of the authorized TFTP server.
ciscoFlashCopySourceName	DisplayString	Name of the billing record file to be transferred, including the Flash device on which it is stored.

Object	Type	Description
ciscoFlashCopyDestinationName	DisplayString	(Optional) Name for the billing record, including path, on the TFTP server. If not specified, the copy operation defaults to saving the billing record at the top-most directory on the TFTP server, using the original file name. **Note** A file with the destination file name should already exist on the TFTP server. This file should be readable and writable by all users, so that it can be replaced with the billing record file.
ciscoFlashCopyProtocol	INTEGER	(Optional) Specifies the protocol to be used when copying the file. For a TFTP transfer, set this object to 1 (tftp), which is the default.
ciscoFlashCopyNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the copy operation. The default is false (no trap is generated).

After transferring the billing records file, you must then set a number of objects in the CISCO-FLASH-MIB to delete the file, so that the Cisco CMTS can begin writing a new file. If the Flash memory is not ATA-compatible, you must also set a number of objects to squeeze the Flash memory to make the deleted space available for new files. Table 229: Deleting a File Using SNMP Commands , on page 1962 describes each of these objects, and whether they are required or optional.

Table 229: Deleting a File Using SNMP Commands

Object	Type	Description
ciscoFlashMiscOpCommand	INTEGER	Specifies the operation to be performed: • 3—Delete the file. • 5—Squeeze the Flash memory, so as to recover the deleted space and make it available for new files.
ciscoFlashMiscOpDestinationName	DisplayString	When deleting a file, the name of the file to be deleted, including the name of the file system, up to a maximum of 255 characters. When squeezing a file system, the name of the file system to be squeezed (slot0:, slot1:, flash:, or bootflash:).

Object	Type	Description
ciscoFlashMiscOpEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashMiscOpNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the operation. The default is false (no trap is generated).

DETAILED STEPS

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Copying the Billing Record File to the TFTP Server

Step 1 The script performing the copy should generate a 32-bit number to be used as the index entry for this copy command. The script can generate this number in any convenient way, so long as the index number is not currently being used for another operation.

Step 2 Create the table entry for the copy command, by using the number that was generated in Step 1 and setting the ciscoFlashCopyEntryStatus object to the create-and-wait state (5):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 5

workstation#
```

Step 3 Set the ciscoFlashCopyCommand to 3 (copyFromFlash) to specify that the billing record file should be copied from the router's Flash file system:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyCommand
.582

-i 3
workstatioN#
```

Step 4 Set the ciscoFlashCopyServerAddress object to the IP address of the TFTP server:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyServerAddress
.582
```

```
-a "172.20.12.193"

workstatioN#
```

Step 5 Set the ciscoFlashCopySourceName object to the file name, including the device name, of the billing record file to be transferred:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopySourceName
.582
-D
"slot0:CMTS01_20030211-155025
"
workstation#
```

Step 6 (Optional) To specify a specific destination on the TFTP server, set the ciscoFlashCopyDestinationName object to the path name and file name for the billing record file on the TFTP server. (Typically, the path name and file name should already exist on the TFTP server.)

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyDestinationName
.582
-D
"/cmts01-billing/billing-file
"
workstation#
```

Step 7 To execute the command, set the ciscoFlashCopyEntryStatus object to the active state (1):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 1

workstation#
```

Step 8 Periodically poll the ciscoFlashCopyStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation#
```

If the file transfer fails, the most common status values that are reported by the ciscoFlashCopyStatus object are:

- 3—copyInvalidOperation. This indicates that the operation failed on the TFTP server, typically because the destination file name and path name do not exist on the TFTP server, or they exist but are not writable by all users.
- 5—copyInvalidSourceName. The file name for the billing record, as specified in ciscoFlashCopySourceName does not exist. Verify that you specified the correct device name and that no spaces exist in the file name.
- 6—copyInvalidDestName. The destination path name and file name specified in ciscoFlashCopyDestinationName is not accessible on the TFTP server. This could be because the path name does not exist or is not configured to

allow write-access. This error could also occur if a file with the same path name and file name already exists on the TFTP server.

- 7—copyInvalidServerAddress. The IP address of the TFTP server specified in ciscoFlashCopyServerAddress is invalid, or the TFTP server is not responding.
- 14—copyFileTransferError. A network error occurred that prevented the file transfer from completing.

Step 9 After the file transfer has completed successfully, set the ciscoFlashCopyEntryStatus object to 6 (delete) to delete the row entry for this copy command:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

What to Do Next

Deleting the Billing Record File

Using SNMP

After the billing record file has been successfully transferred, use the following procedure to delete the billing record on the Cisco CMTS flash file system, so that the Cisco CMTS can write the new billing record.

Step 1 Generate another random number to be used as an index entry and configure the following objects in the ciscoFlashMiscOpTable:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation#
```

Step 2 Periodically poll the ciscoFlashMiscOpStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
```

```
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation#
```

Step 3 If the Flash memory system is not ATA-compatible (slot0:, slot1:, flash:, or bootflash:), configure the following objects in the ciscoFlashMiscOpTable to squeeze the Flash file system to recover the deleted file space:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 1

workstation#
```

Examples To Transfer Using SNMP

The following SNMP commands transfer a file named CMTS01_20030211-155025 to a TFTP server at the IP address 10.10.31.3. After the file is successfully transferred, the row entry for this copy command is deleted.

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyCommand
.582
 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyServerAddress
.582
 -a "10.10.31.3"

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopySourceName
.582 -D
"slot0:CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyDestinationName
.582 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
```

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

The following commands show a billing record file being deleted on the Cisco CMTS file system, and the deleted file space being recovered by a squeeze operation:

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 1

workstation#
```

Disabling the Usage-based Billing Feature

This section describes how to disable the Usage-based Billing. Giving this command immediately stops the collection of billing information. If a billing record is currently written or being streamed to an external server, the CMTS completes the operation before disabling the usage-based billing feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router#`	
Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 3	**no cable metering** **Example:** `Router(config)# no cable metering` **Example:** `Router(config)#`	Immediately disables the Usage-based Billing feature and stops the collection of billing information.
Step 4	**no snmp-server enable traps cable metering** **Example:** `Router(config)# no snmp-server enable traps cable metering` **Example:** `Router(config)#`	(Optional) Disables SNMP traps for usage-based billing events.
Step 5	**no cable sflog** **Example:** `Router(config)# no cable sflog` **Example:** `Router(config)#`	(Optional) Disables the logging of deleted service flows.
Step 6	**no cable metering source-interface** **Example:** `Router(config)# no cable metering source-interface`	(Optional) Disables a specified source-interface for the billing packets.

	Command or Action	Purpose
	Example: `Router(config)#`	
Step 7	**exit** **Example:** `Router(config)# exit` **Example:** `Router#`	Exits global configuration mode.

Configuring Certified SSL Servers for Usage-Based Billing

Cisco IOS Release 12.3(17a)BC introduces support for the Secure Socket Layer (SSL) Server, used with the usage-based billing feature of the Cisco CMTS. Usage-based billing implements the DOCSIS Subscriber Account Management Interface Specification (SAMIS) format.

This new capability enables the configuration of the SSL server between the Cisco CMTS and a collection server. Certificate creation steps and **debug** commands are added or enhanced to support the SSL Server and certificates. This section describes general steps.

Refer also to the "Configuring the Cisco CMTS for SSL Operation" section .

Generating SSL Server Certification

These general steps describe the creation and implementation of certification for the Secure Socket Layer (SSL) Server.

1. Generate the CA key.
2. Set up the open SSL environment, to include directory and sub-directory.
3. Copy files to the appropriate directories.
4. Generate the SSL Server certification request.
5. Grant the SSL Server certification request.
6. Convert the SSL Server certification to DER format.
7. Copy the SSL certification to Bootflash memory (write mem).
8. Start the SSL server.

Configuring and Testing the Cisco CMTS for Certified SSL Server Support

Perform the following steps to configure the Cisco router to support the SSL Server and certification.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip domain name** *domain* **Example:** `Router(config)# ip domain name Cisco.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. **Note** See the Domain Name System (DNS) document on Cisco.com for additional DNS information.
Step 4	**crypto key generate rsa** **Example:** `Router(config)# crypto key generate rsa`	Generates RSA key pairs.
Step 5	Ctrl-Z **Example:** `Router(config)# Ctrl-Z` **Example:** `Router#`	Returns to privileged EXEC mode.
Step 6	**test cable read certificate** **Example:** `Router# test cable read certificate`	Verifies the certificate is valid and operational on the Cisco CMTS.
Step 7	**show crypto ca certificate** **Example:** `Router# show crypto ca certificate`	Displays the available certificates on the Cisco CMTS.

	Command or Action	Purpose
Step 8	**configure terminal** **Example:** `Router# configure terminal` **Example:** `Router(config)#`	Enters global configuration mode.
Step 9	**cable metering destination** *ip-addr num-1 num-2 num-3* **secure** **Example:** `Router(config)# cable metering destination 1.7.7.7 6789 0 15 secure`	Defines the destination IP address for cable metering, to be used with the certificate.
Step 10	test cable metering **Example:** `Router# test cable metering`	Tests cable metering in light of the supported SSL server and metering configuration.

Monitoring the Usage-based Billing Feature

To display the most current billing record, use the **show cable metering-status** command. The following example shows typical output when usage-based billing is configured to write the billing records to a local file system:

```
CMTS01# show cable metering-status

destination                          complete-time   flow   cpe     status
                                                     aggr suppress
disk0:R7519-UBR7246-20000308-004428 Jun 12 09:33:05  No     No     success
CMTS01#
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to stream the billing records to an external server:

```
Router# show cable metering-status

destination                       complete-time   flow cpe  full status
                                                  aggr supp rec
10.11.37.2 :1234                  Jun 12 09:33:05  No   No  No success
Router#
```

The following example shows a typical output for the **show cable metering-status** command using verbose option:

```
Router# show cable metering-status verbose
```

```
Last export status
Destination : disk0:sunethra10k-20070129-190423
Complete Time : Jan29 19:04:38
Flow Aggregate : No
Full records : No
Cpe list suppression : No
Source interface : FastEthernet0/0/0
Status of last export : success
Current export status : In progress
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
destination                complete-time   flow  cpe   full    status
             aggr  supp  rec
IPDR_Session2               Apr12 16:51:15  No    No    No    success
```

The following example shows a typical output for the verbose form of the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
 verbose

Last export status
Destination               : IPDR_Session2
Complete Time          : Apr12 16:51:15
Flow Aggregate         : No
Full records               :No
Cpe list suppression   : No
Source interface       : Not defined
Status of last export  : success
```

Note If the **show cable metering-status** command displays the status of a streaming operation as "success" but the records were not received on the billing application server, verify that the Cisco CMTS and server are configured for the same type of communications (non-secure TCP or secure SSL). If the Cisco CMTS is configured for non-secure TCP and the server is configured for secure SSL, the Cisco CMTS transmits the billing record successfully, but the server discards all of the data, because it did not arrive in a secure SSL stream.

Tip The **show cable metering-status** command continues to show the status of the last billing record operation, until that billing record is deleted. If the record is not deleted, no new records are created.

To display information about the state of the IPDR Exporter, use the show ipdr Exporter command. The following example shows typical output:

```
Router#configure terminal
Router#show ipdr exporter
```

IPDR exporter is started.

Configuration Examples for Usage-based Billing

This section lists the following sample configurations for the Usage-based Billing feature:

File Mode Configuration (with Secure Copy)

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in file mode and enabling Secure Copy (SCP) for file transfers.

```
!
cable metering filesystem disk1:
snmp-server enable traps cable metering
...
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
username billingapp level 15 password 7 billing-password
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

Non-Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying both a primary and a secondary external server. The data is sent using standard TCP packets, without any security.

```
cable metering destination 10.10.10.171 5321 10.10.10.173 5321 2 30 non-secure
snmp-server enable traps cable metering
```

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server:

```
cable metering destination 10.10.11.181 6789 2 30 non-secure
snmp-server enable traps cable metering
```

Note You must ensure that the billing application server is configured for standard TCP communications. If the billing application server is configured for SSL communications when the Cisco CMTS is configured for standard TCP, the Cisco CMTS is able to send the billing records to the server, but the server discards all of that information because it is not arriving in a secure stream.

Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server. Secure socket layer (SSL) TCP connections are used to transmit the data, which requires the configuration of a digital certificate.

```
cable metering destination 10.10.11.181 6789 2 30 secure cpe-list-suppress
snmp-server enable traps cable metering
...
crypto ca trustpoint SSL-CERT
!
crypto ca certificate chain SSL-CERT
 certificate ca 00
  308204A6 3082038E A0030201 02020100 300D0609 2A864886 F70D0101 04050030
  8198310B 30090603 55040613 02555331 13301106 03550408 130A4361 6C69666F
  726E6961 3111300F 06035504 07130853 616E204A 6F736531 1C301A06 0355040A
  13134369 73636F20 53797374 656D732C 20496E63 2E311130 0F060355 040B1308
  4361626C 65204255 310E300C 06035504 03130553 65656D61 3120301E 06092A86
...
```

```
  3E65DBBA 337627E8 589980D6 C8836C7E 3D3C3BC1 F21973BF 7B287D7A 13B16DA2
  02B2B180 C2A125C7 368BDA4C 0B8C81B7 7D5BEFF9 A6618140 1E95D19E BD0A84F5
  B43702AB 39B5E632 87BA36AC A3A8A827 C5BAC0F1 B24B8F4D 55615C49 5B6E4B61
  B15CC48A 8EF566C8 6E449B49 BF8E9165 317C1734 9A48A240 78A356B5 403E9E9B
  88A51F5B 0FE38CC2 F431
  quit
!
```

Note You must ensure that the billing applications server is also configured for SSL communications.

Feature Information for Usage-Based Billing for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Note The table lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

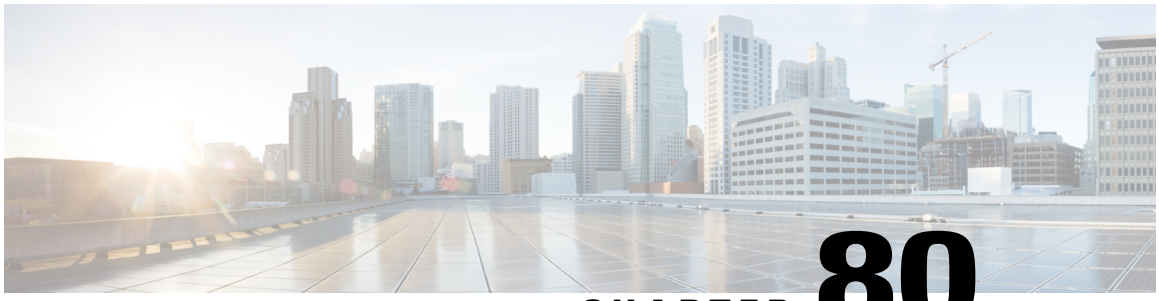
Table 230: Feature Specifications for Usage-based Billing

Feature Name	Release	Feature Information
Usage-based Billing	12.3(9a)BC	This feature was introduced on Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers. Feature support includes the new CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format.

Feature Name	Release	Feature Information
Usage-based Billing	12.3(17a)BC	This feature includes additional MIBs that support OSSI specifications as well as enhanced billing reports. For more information about DOCSIS 2.0, see the Cable Labs document Data-Over-Cable Service Interface Specifications DOCSIS 2.0 Operations Support System Interface Specification. Support for Secure Socket Layer (SSL) Servers introduced with certification support.
Usage-based Billing	12.3(21)BC	This feature provides enhancements to specify the source interface for billing packets in the Subscriber Account Management Interface Specification (SAMIS). The cable metering source-interface <interface> command was introduced. Support also includes a new object **ccmtrCollectionSrcIfIndex** in CISCO-CABLE-METERING-MIB.my.
Usage-based Billing	12.2(33)SCB	SAMIS over Internet Protocol Detail Record (IPDR) was introduced.
Usage-based Billing	12.2(33)SCC4 12.2(33)SCD2	Added the **full-records** keyword to the **cable metering** commands. Introduced the **cable util-interval** command.
Usage-based Billing	12.2(33)SCI2	Added the**localtime** keyword in the **cable metering** command to enable local time timestamping in the IPDRcreationTime field in the Billing records.

PART XI

Configuration Register and Frequency Allocation Information



CHAPTER 80

Configuration Register Information for the Cisco CMTS Routers

This document provides the following information:

Configuration Bit Meanings

Use the processor configuration register information contained in this section to do the following:

- Set and display the configuration register value
- Force the system into the bootstrap program
- Select a boot source and default boot filename
- Enable or disable the Break function
- Control broadcast addresses
- Set the console terminal baud rate
- Load operating software from ROM
- Enable booting from a Trivial File Transfer Protocol (TFTP) server

The table below lists the meaning of each of the configuration memory bits:

Table 231: Configuration Register Bit Settings

Bit Number	Hex	Meaning
00–03	0x0000–0x000F	Boot field
06	0x0040	Causes the system software to ignore nonvolatile random-access memory (NVRAM) contents
07	0x0080	OEM (original equipment manufacturer) bit enabled
08	0x0100	Break disabled
10	0x0400	IP broadcast with all zeros
11–12	0x800–0x1000	Console line speed
13	0x2000	Boots default ROM software if initial boot fails
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enables diagnostic messages and ignores NVRAM contents

Bits 0–3

The lowest four bits of the processor configuration register (bits 3, 2, 1, and 0) form the boot field.

The table below provides information about the bits settings:

Table 232: Bits 0–3 Settings

Boot Field	Meaning
0	Stays at the system bootstrap prompt (ROM monitor) on a reload or power cycle
1	Boots the boot helper image as a system image
2	Full boot process, which loads the Cisco IOS image into Flash memory
2-F	Specifies a default filename for booting over the network from a TFTP server

The boot field specifies a number in binary. If you set the boot field value to 0, you must have a console port access to boot the operating system manually. Boot the operating system by entering the **b** command at the bootstrap prompt as follows:

```
> b [tftp] flash filename
```

Definitions of the various command options follow:

b—Boots the default system software from ROM

b flash—Boots the first file in Flash memory

b *filename* [*host*]**—**Boots over the network using TFTP

b flash *filename***—**Boots the file (filename) from Flash memory

If you set the boot field value to a value of 2 through F, and there is a valid system boot command stored in the configuration file, the router boots the system software as directed by that value. (See Table 233: Default Boot Filenames, on page 1981) If you set the boot field to any other bit pattern, the router uses the resulting number to form a default boot filename for netbooting.

If there are no boot commands in the configuration file, the router attempts to boot the first file in system Flash memory. If no file is found in system Flash memory, the router attempts to netboot a default file with a name derived from the value of the boot field (for example, cisco2-7200). If the netboot attempt fails, the boot helper image in boot flash memory will boot up.

If **boot** commands are in the configuration file, the router software processes each **boot** command in sequence until the process is successful or the end of the list is reached. If the end of the list is reached without a file being successfully booted, the router will retry the **netboot** commands up to six times if bit 13 of the configuration register is set, otherwise it will load the operating system software available in ROMmon. If bit 13 is not set, the router will continue to netboot images indefinitely. The default setting for bit 13 is 0. If bit 13 is set, the system boots the boot helper image found in boot flash memory without any retries.

The server creates a default filename as part of the automatic configuration processes. To form the boot filename, the server starts with Cisco and links the octal equivalent of the boot field number, a dash, and the image name.

Note A **boot system configuration** command in the router configuration in NVRAM overrides the default netboot filename.

The table below lists the default boot filenames or actions:

Table 233: Default Boot Filenames

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
ROM software	0	0	0	1
Flash software	0	0	1	0
cisco3-< image-name1>	0	0	1	1
cisco4-<image-name2>	0	1	0	0

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
cisco5-<image-name3>	0	1	0	1
cisco6-<image-name4>	0	1	1	0
cisco7-<image-name5>	0	1	1	1
cisco10-<image-name6>	1	0	0	0
cisco11-<image-name7>	1	0	0	1
cisco12-<image-name8>	1	0	1	0
cisco13-<image-name9>	1	0	1	1
cisco14-<image-name10>	1	1	0	0
cisco15-<image-name11>	1	1	0	1
cisco16-<image-name12>	1	1	1	0
cisco17-<image-name13>	1	1	1	1

Bit 6

Bit 6 causes the system software to ignore nonvolatile random-access memory (NVRAM) contents.

Bit 7

Bit 7 enables the OEM bit. It disables the bootstrap messages at startup.

Bit 8

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret Break as a command to force the system into the bootstrap monitor, halting normal operation. A Break can be sent in the first sixty seconds while the system reboots, regardless of the configuration settings.

Bit 10 and Bit 14

Bit 10 controls the host portion of the Internet IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. B it 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address. The table below shows the combined effect of bit 10 and bit 14:

Table 234: Bit 10 and Bit 14 Settings

Bit 14	Bit 10	IP Address (<net> <host>)
Off	Off	<ones><ones>
Off	On	<zeros><zeros>
On	On	<net><zeros>
On	Off	<net><ones>

Note The console line rate on Cisco universal broadband routers is fixed at 9600 and cannot be changed. For more information about configuring baud rates, see *Appendix B: Cisco CMTS Router ROM Monitor Commands* in the Cisco IOS CMTS Cable Command Reference .

Bit 11 and Bit 12

Bit 11 and Bit 12 in the configuration register determine the baud rate of the console terminal. The table below shows the bit settings for the four available baud rates (the factory set default baud rate is 9600):

Table 235: Bit 11 and Bit 12 Settings

Baud	Bit 12	Bit 11
9600	0	0
4800	0	1
2400	1	1
1200	1	0

Note The console line rate on Cisco universal broadband routers is fixed at 9600 and cannot be changed. For more information about configuring baud rates, see *Appendix B: Cisco CMTS Router ROM Monitor Commands* in the Cisco IOS CMTS Cable Command Reference .

Bit 13

Bit 13 determines the server response to a bootload failure. If **boot** commands are in the configuration file, the router software processes each **boot** command in sequence until the process is successful or the end of the list is reached. If the end of the list is reached without a file being successfully booted, the router will retry the **netboot** commands up to six times if bit 13 of the configuration register is set, otherwise it will load the

operating system software available in ROMmon. If bit 13 is not set, the router will continue to netboot images indefinitely. The default setting for bit 13 is 0. If bit 13 is set, the system boots the boot helper image found in boot flash memory without any retries.

Bit 15

Bit 15 enables diagnostic messages and ignores NVRAM contents.

Examples for Displaying the Configuration Register While Running Cisco IOS

This section provides examples for displaying the configuration register for while running Cisco IOS on Cisco uBR10012 and Cisco uBR7200 series routers.

Example: Displaying the Configuration Register While Running Cisco IOS on a Cisco uBR10012 Router

The configuration register can be viewed by using the **show version** or **show hardware** command.

The following example illustrates output from the **show version** command for a Cisco uBR10012 router with the Cisco OC-48 DPT/POS interface module in POS mode:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K-K8P6-M), Experimental Version 12.2(20021115:194156)
[REL-ftp_p2_clip
per_srp.ios-weekly 103]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 15-Nov-02 18:05 by richv
Image text-base: 0x60008940, data-base: 0x61A80000

ROM: System Bootstrap, Version 12.0(9r)SL2, RELEASE SOFTWARE (fc1)

R7582-ubr10k-UUT uptime is 10 hours, 14 minutes
System returned to ROM by power-on
System image file is "bootflash:ubr10k-k8p6-mz.oc48.15Nov02"

cisco uBR10012 (PRE1-RP) processor with 393215K/131072K bytes of memory.
Processor board ID TBA05080267
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
Backplane version 1.0, 8 slot

Last reset from power-on
Toaster processor tmc0 is running.
Toaster processor tmc1 is running.
1 OC12 POS controller (1 POS)
1 TCCplus card(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Gigabit Ethernet/IEEE 802.3 interface(s)
3 Packet over SONET network interface(s)
2 Cable Modem network interface(s)
509K bytes of non-volatile configuration memory.

46976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
32768K bytes of Flash internal SIMM (Sector size 256KB).
Configuration register is 0x0

Router#
```

Example: Displaying the Configuration Register While Running Cisco IOS on a Cisco uBR7200 Series Router

The configuration register can be viewed by using the **show version** or **show hardware** command.

The following example illustrates output from the **show version** command for a Cisco uBR7246 VXR router with the cable clock card installed:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-P-M), Version 12.1(10)EC, RELEASE SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 02-Feb-00 16:49 by ccai
Image text-base:0x60008900, data-base:0x61192000

ROM:System Bootstrap, Version 12.0(15)SC, RELEASE SOFTWARE

VXR1 uptime is 2 days, 1 hour, 24 minutes
System returned to ROM by power-on at 10:54:38 PST Sat Feb 5 2000
System restarted at 11:01:08 PST Sat Feb 5 2000
System image file is "slot1:ubr7200-p-mz.121-0.8.T"

cisco uBR7246VXR (NPE300) processor (revision B) with 122880K/40960K bytes of memory.
Processor board ID SAB0329005N
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0

Last reset from power-on
X.25 software, Version 3.0.0.
National clock card with T1 controller
1 FastEthernet/IEEE 802.3 interface(s)
2 Cable Modem network interface(s)
125K bytes of non-volatile configuration memory.

16384K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0

Router#
```

Example: Displaying the Configuration Register While Running ROM Monitor

If the bootstrap prompt ">", the **o** command displays the virtual configuration register currently in effect. It includes a description of the bits. See the following sample output:

```
>o

Configuration register + 02x100 at last boot
Bit#        Configuration register option settings:
15         Diagnostic mode disabled
14         IP broadcasts do not have network numbers
13         Boot default ROM software if network boot fails
12-11      Console speed is 9600 baud
10         IP broadcasts with ones
09         Do not use secondary bootstrap
08         Break disabled
07         OEM disabled
06         Ignore configuration disabled
05         Fast boot disabled
04         Fan boot disabled
03-00      Boot to ROM monitor
```

If the prompt is "rommon1", the **confreg** command displays the virtual configuration register currently in effect. It includes a description of the bits. See the following sample output:

```
rommon 1 > confreg

Configuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: the ROM Monitor

Do you wish to change the configuration? y/n  [n]
```

Example: Setting the Configuration Register While Running Cisco IOS

The configuration register can be set in the configuration mode with the **config-register 0x** *value* command. See the following sample output:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)# config-register 0x2142
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Example: Setting the Configuration Register While Running ROM Monitor

If the prompt is ">", the **or0x** *value* command sets the configuration register. See the following sample output:

```
>o/r 0x2102
>
```

If the prompt is "rommon1", the **confreg** command sets the configuration register. It prompts the user about each bit. See the following sample output:

```
rommon 1 > confreg

Confiuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration y/n    [n]:  y
enable  "diagnostic mode"? y/n   [n]:   n
enable   "use net in IP bcast address"? y/n  [n]:   n
disable  "use rom after netboot fails"? y/n  [n]:  n
enable   "use all zero broadcast"? y/n  [n]:  n
enable   "break/abort has effect"? y/n  [n]:  n
enable   "ignore system config info"? y/n   [n]:  n
change console baud rate? y/n  [n]:  n
change the boot characteristics? y/n   [n]:y
enter to boot:
0 = ROM Monitor
1 = the boot helper image
2 - 15 = boot system
[0]: 2

Configuration Summary:
enabled are:
load rom after netboot fails
console baud: 9600
boot: image sepcified by the boot system commands or default to: cisco2-c7200

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

```
You must reset or power cycle for new config to take effect
rommon 2 >
```

CHAPTER 81

Frequency Allocation Information for the Cisco CMTS Routers

Frequency Allocation for the Cisco CMTS Routers

The table below provides information about the NTSC 6-MHz channel bands:

Table 236: NTSC Cable Television Channels and Relative Frequencies in MHz

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
T 7	5.75 - 11.75	7	10.58	11.5
T 8	11.75 - 17.75	13	16.58	17.5
T9	17.75-23.75	19	22.58	23.5
T10	23.75-29.75	25	28.58	29.5
T11	29.75-35.75	31	34.58	35.5
T12	35.75-41.75	37	40.58	41.5
T13	41.75-47.75	43	46.58	47.5
TV-IF	40.0-46.0	45.75	42.17	41.25
2-2	54.0-60.0	55.25	58.83	59.75
3-3	60.0-66.0	61.25	64.83	65.75
4-4	66.0-72.0	67.25	70.83	71.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
5-5	76.0-82.0	77.25	80.83	81.75
6-6	82.0-88.0	83.25	86.83	87.75
FM	88.0-108.0			
A-5-95	90.0-96.0	91.25	94.83	95.75
A-4-96	96.0-102.0	97.25	100.83	101.75
A-3-97	102.0-108.0	103.25	106.83	107.75
A-2-98	108.0-114.0	109.25	112.83	113.75
A-1-99	114.0-120.0	115.25	118.83	119.75
A-14	120.0-126.0	121.25	124.83	125.75
B-15	126.0-132.0	127.25	130.83	131.75
C-16	132.0-138.0	133.25	136.83	137.75
D-17	138.0-144.0	139.25	142.83	143.75
E-18	144.0-150.0	145.25	148.83	149.75
F-19	150.0-156.0	151.25	154.83	155.75
G-20	156.0-162.0	157.25	160.83	161.75
H-21	162.0-168.0	163.25	166.83	167.75
I-22	168.0-174.0	169.25	172.83	173.75
7-7	174.0-180.0	175.25	178.83	179.75
8-8	180.0-186.0	181.25	184.83	185.75
9-9	186.0-192.0	187.25	190.83	191.75
10-10	192.0-198.0	193.25	196.83	197.75
11-11	198.0-204.0	199.25	202.83	203.75
12-12	204.0-210.0	205.25	208.83	209.75
13-13	210.0-216.0	211.25	214.83	215.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
J-23	216.0-222.0	217.25	220.83	221.75
K-24	222.0-228.0	223.25	226.83	227.75
L-25	228.0-234.0	229.25	232.83	233.75
M-26	234.0-240.0	235.25	238.83	239.75
N-27	240.0-246.0	241.25	244.83	245.75
O-28	246.0-252.0	247.25	250.83	251.75
P-29	252.0-258.0	253.25	256.83	257.75
Q-30	258.0-264.0	259.25	262.83	263.75
R-31	264.0-270.0	265.25	268.83	269.75
S-32	270.0-276.0	271.25	274.83	275.75
T-33	276.0-282.0	277.25	280.83	281.75
U-34	282.0-288.0	283.25	286.83	287.75
V-35	288.0-294.0	289.25	292.83	293.75
W-36	294.0-300.0	295.25	298.83	299.75
AA-37	300.0-306.0	301.25	304.83	305.75
BB-38	306.0-312.0	307.25	310.83	311.75
CC-39	312.0-318.0	313.25	316.83	317.75
DD-40	318.0-324.0	319.25	322.83	323.75
EE-41	324.0-330.0	325.25	328.83	329.75
FF-42	330.0-336.0	331.25	334.83	335.75
GG-43	336.0-342.0	337.25	340.83	341.75
HH-44	342.0-348.0	343.25	346.83	347.75
II-45	348.0-354.0	349.25	352.83	353.75
JJ-46	354.0-360.0	355.25	358.83	359.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
KK-47	360.0-366.0	361.25	364.83	365.75
LL-48	366.0-372.0	367.25	370.83	371.75
MM-49	372.0-378.0	373.25	376.83	377.75
NN-50	378.0-384.0	379.25	382.83	383.75
OO-51	384.0-390.0	385.25	388.83	389.75
PP-52	390.0-396.0	391.25	394.83	395.75
QQ-53	396.0-402.0	397.25	400.83	401.75
RR-54	402.0-408.0	403.25	406.83	407.75
SS-55	408.0-414.0	409.25	412.83	413.75
TT-56	414.0-420.0	415.25	418.83	419.75
UU-57	420.0-426.0	421.25	424.83	425.75
VV-58	426.0-432.0	427.25	430.83	431.75
WW-59	432.0-438.0	433.25	436.83	437.75
XX-60	438.0-444.0	439.25	442.83	443.75
YY-61	444.0-450.0	445.25	448.83	449.75
ZZ-62	450.0-456.0	451.25	454.83	455.75
AAA-63	456.0-462.0	457.25	460.83	461.75
BBB-64	462.0-468.0	463.25	466.83	467.75
CCC-65	468.0-474.0	469.25	472.83	473.75
DDD-66	474.0-480.0	475.25	478.83	479.75
EEE-67	480.0-486.0	481.25	484.83	485.75
FFF-68	486.0-492.0	487.25	490.83	491.75
GGG-69	492.0-498.0	493.25	496.83	497.75
HHH-70	498.0-504.0	499.25	502.83	503.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
III-71	504.0-510.0	505.25	508.83	509.75
JJJ-72	510.0-516.0	511.25	514.83	515.75
KKK-73	516.0-522.0	517.25	520.83	521.75
LLL-74	522.0-528.0	523.25	526.83	527.75
MMM-75	528.0-534.0	529.25	532.83	533.75
NNN-76	534.0-540.0	535.25	538.83	539.75
OOO-77	540.0-546.0	541.25	544.83	545.75
PPP-78	546.0-552.0	547.25	550.83	551.75
QQQ-79	552.0-558.0	553.25	556.83	557.75
RRR-80	558.0-564.0	559.25	562.83	563.75
SSS-81	564.0-570.0	565.25	568.83	569.75
TTT-82	570.0-576.0	571.25	574.83	575.75
UUU-83	576.0-582.0	577.25	580.83	581.75
VVV-84	582.0-588.0	583.25	586.83	587.75
WWW-85	588.0-594.0	589.25	592.83	593.75
XXX86	594.0-600.0	595.25	598.83	599.75
YYY-87	600.0-606.0	601.25	604.83	605.75
ZZZ-88	606.0-612.0	607.25	610.83	611.75
89-89	612.0-618.0	613.25	616.83	617.75
90-90	618.0-624.0	619.25	622.83	623.75
91-91	624.0-630.0	625.25	628.83	629.75
92-92	630.0-636.0	631.25	634.83	635.75
93-93	636.0-642.0	637.25	640.83	641.75
94-94	642.0-648.0	643.25	646.83	647.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
100-100	648.0-654.0	649.25	652.83	653.75
101-101	654.0-660.0	655.25	658.83	659.75
102-102	660.0-666.0	661.25	664.83	665.75
103-103	666.0-672.0	667.25	670.83	671.75
104-104	672.0-678.0	673.25	676.83	677.75
105-105	678.0-684.0	679.25	682.83	683.75
106-106	684.0-690.0	685.25	688.83	689.75
107-107	690.0-696.0	691.25	694.83	695.75
108-108	696.0-702.0	697.25	700.83	701.75
109-109	702.0-708.0	703.25	706.83	707.75
110-110	708.0-714.0	709.25	712.83	713.75
111-111	714.0-720.0	715.25	718.83	719.75
112-112	720.0-726.0	721.25	724.83	725.75
113-113	726.0-732.0	727.25	730.83	731.75
114-114	732.0-738.0	733.25	736.83	737.75
115-115	738.0-744.0	739.25	742.83	743.75
116-116	744.0-750.0	745.25	748.83	749.75
117-117	750.0-756.0	751.25	754.83	755.75
118-118	756.0-762.0	757.25	760.83	761.75
119-119	762.0-768.0	763.25	766.83	767.75
120-120	768.0-674.0	769.25	772.83	773.75
121-121	774.0-780.0	775.25	778.83	779.75
122-122	780.0-786.0	781.25	784.83	785.75
123-123	786.0-792.0	787.25	790.83	791.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
124-124	792.0-798.0	793.25	796.83	797.75
125-125	798.0-804.0	799.25	802.83	803.75
126-126	804.0-810.0	805.25	808.83	809.75
127-127	810.0-816.0	811.25	814.83	815.75
128-128	816.0-822.0	817.25	820.83	821.75
129-129	822.0-828.0	823.25	826.83	827.75
130-130	828.0-834.0	829.25	832.83	833.75
131-131	834.0-840.0	835.25	838.83	839.75
132-132	840.0-846.0	841.25	844.83	845.75
133-133	846.0-852.0	847.25	850.83	851.75
134-134	852.0-858.0	853.25	856.83	857.75
135-135	858.0-864.0	859.25	862.83	863.75
136-136	864.0-870.0	865.25	868.83	869.75
137-137	870.0-876.0	871.25	874.83	875.75
138-138	876.0-882.0	877.25	880.83	881.75
139-139	882.0-888.0	883.25	886.83	887.75
140-140	888.0-894.0	889.25	892.83	893.75
141-141	894.0-900.0	895.25	898.83	899.75
142-142	900.0-906.0	901.25	904.83	905.75
143-143	906.0-912.0	907.25	910.83	911.75
144-144	912.0-918.0	913.25	916.83	917.75
145-145	918.0-924.0	919.25	922.83	923.75
146-146	924.0-930.0	925.25	928.83	929.75
147-147	930.0-936.0	931.25	934.83	935.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
148-148	936.0-942.0	937.25	940.83	941.75
149-149	942.0-948.0	943.25	946.83	947.75
150-150	948.0-954.0	949.25	952.83	953.75
151-151	954.0-960.0	955.25	958.83	959.75
152-152	960.0-966.0	961.25	964.83	965.75
153-153	966.0-972.0	967.25	970.83	971.75
154-154	972.0-978.0	973.25	976.83	977.75
155-155	978.0-984.0	979.25	982.83	983.75
156-156	984.0-990.0	985.25	988.83	989.75
157-157	990.0-996.0	991.25	994.83	995.75
158-158	996.0-1002.0	997.25	1000.83	1001.75

The table below provides information on the Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) 8-MHz channel bands:

Table 237: European Cable Television Channels and Relative Frequencies in MHz

Channel Number	Bandwidth	Video Carrier	Audio Carrier
2	47-54	48.25	48.25
3	54-61	55.25	55.25
4	61-68	62.25	62.25
S2	111-118	112.25	112.25
S3	118-125	119.25	119.25
S4	125-132	126.25	126.25
S5	132-139	133.25	133.25
S6	139-146	140.25	140.25
S7	146-153	147.25	147.25
S8	153-160	154.25	154.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
S9	160-167	161.25	161.25
S10	167-174	168.25	168.25
5	174-181	175.25	175.25
6	181-188	182.25	182.25
7	188-195	189.25	189.25
8	195-202	196.25	196.25
9	202-209	203.25	203.25
10	209-216	210.25	210.25
11	216-223	217.25	217.25
12	223-230	224.25	224.25
S11	230-237	231.25	231.25
S12	237-244	238.25	238.25
S13	244-251	245.25	245.25
S14	251-258	252.25	252.25
S15	258-265	259.25	259.25
S16	265-272	266.25	266.25
S17	272-279	273.25	273.25
S18	279-286	280.25	280.25
S19	286-293	287.25	287.25
S20	293-300	294.25	294.25
S21	302-310	303.25	303.25
S22	310-318	311.25	311.25
S23	318-326	319.25	319.25
S24	326-334	327.25	327.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
S25	334-342	335.25	335.25
S26	342-350	343.25	343.25
S27	350-358	351.25	351.25
S28	358-366	359.25	359.25
S29	366-374	367.25	367.25
S30	374-382	375.25	375.25
S31	382-390	383.25	383.25
S32	390-398	391.25	391.25
S33	398-406	399.25	399.25
S34	406-414	407.25	407.25
S35	414-422	415.25	415.25
S36	422-430	423.25	423.25
S37	430-438	431.25	431.25
S38	438-446	439.25	439.25
21	470-478	471.25	471.25
22	478-486	479.25	479.25
23	486-494	487.25	487.25
24	494-502	495.25	495.25
25	502-510	503.25	503.25
26	510-518	511.25	511.25
27	518-526	519.25	519.25
28	526-534	527.25	527.25
29	534-542	535.25	535.25
30	542-550	543.25	543.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
31	550-558	551.25	551.25
32	558-566	559.25	559.25
33	566-574	567.25	567.25
34	574-582	575.25	575.25
35	582-590	583.25	583.25
36	590-598	591.25	591.25
37	598-606	599.25	599.25
38	606-614	607.25	607.25
39	614-622	615.25	615.25
40	622-630	623.25	623.25
41	630-638	631.25	631.25
42	638-646	639.25	639.25
43	646-654	647.25	647.25
44	654-662	655.25	655.25
45	662-670	663.25	663.25
46	670-678	671.25	671.25
47	678-686	679.25	679.25
48	686-694	687.25	687.25
49	694-702	695.25	695.25
50	702-710	703.25	703.25
51	710-718	711.25	711.25
52	718-726	719.25	719.25
53	726-734	727.25	727.25
54	734-742	735.25	735.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
55	742-750	743.25	743.25
56	750-758	751.25	751.25
57	758-766	759.25	759.25
58	766-774	767.25	767.25
59	774-782	775.25	775.25
60	782-790	783.25	783.25
61	790-798	791.25	791.25
62	798-806	799.25	799.25
63	806-814	807.25	807.25
64	814-822	815.25	815.25
65	822-830	823.25	823.25
66	830-838	831.25	831.25
67	838-846	839.25	839.25
68	846-854	847.25	847.25
69	854-862	855.25	855.25