



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, page 2](#)
- [Activating Downstream Cable Address Resolution Protocol Requests, page 3](#)
- [Activating Downstream Ports, page 5](#)
- [Assigning the Downstream Channel ID, page 6](#)
- [Traffic Shaping, page 7](#)
- [Configuring Downstream Rate Limiting and Traffic Shaping, page 8](#)
- [Setting the Downstream Helper Address, page 9](#)
- [Setting the Downstream Interleave Depth, page 10](#)
- [Setting the Downstream Modulation, page 11](#)
- [Setting the Downstream MPEG Framing Format, page 12](#)
- [Setting Downstream Traffic Shaping, page 12](#)
- [Activating Host-to-Host Communication \(Proxy ARP\), page 14](#)
- [Activating Packet Intercept Capabilities, page 15](#)
- [Configuring Payload Header Suppression and Restoration, page 15](#)
- [Setting Optional Broadcast and Cable IP Multicast Echo, page 16](#)
- [Cable Interface Configuration Examples, page 18](#)

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 1: 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 <ul style="list-style-type: none"> • PRE-2 Cisco IOS Release 12.2(33)SCH and later releases <ul style="list-style-type: none"> • PRE5 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • NPE-G1 • NPE-G2 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • NPE-G1 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	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 Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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
<pre>Router(config-if)# [no] cable downstream rate-limit token-bucket [shaping] weighted-discard [expwt <n>]</pre>	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 msec.
- 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 msec.
- 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	<p>cable downstream rate-limit token-bucket [shaping [granularity msec max-delay msec]</p> <p>Example: Router(config-if)# cable downstream rate-limit token-bucket</p> <p>Router(config-if)# cable downstream rate-limit token-bucket shaping</p> <p>Router(config-if)# cable downstream rate-limit token-bucket shaping granularity 8</p> <p>Router(config-if)# cable downstream rate-limit token-bucket shaping max-delay 256</p>	<p>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.</p> <p>Enables traffic shaping on the downstream port using the token bucket policing algorithm with traffic shaping.</p> <p>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.</p> <p>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.</p>
Step 2	<p>cable downstream rate-limit weighted-discard <i>exp-weight</i></p> <p>Example: Router(config-if)# cable downstream rate-limit weighted-discard 3</p>	<p>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.</p>
Step 3	<p>end</p> <p>Example: Router(config-if)# end</p>	<p>Exits back to privileged EXEC mode so that you can verify the steps.</p>

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 xxx.xxxx.xxx	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 xxx.xxxx.xxx	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
<code>show interface cable x/0/0 service-flow [sfid] phs</code>	Displays cable interface information.
<code>debug cable error</code>	Displays errors that occur in the cable MAC protocols. To disable debugging output, use the no form of the command.
<code>debug cable phs</code>	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
<code>Router(config-if)# cable ip-multicast-echo</code>	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 ispl
!
! 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:

```
Router(config-router)# neighbor 200.28.28.40 activate
```


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 IPv4 address 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
```
