Cable Commands: cable e through cable i

Revised: May 2013, OL-15510-16

New Commands

Command	Cisco IOS Software Release
cable ip-init	12.2(33)SCA
cable ipv6 source-verify	12.2(33)SCA
cable init-channel-timeout	12.2(33)SCC
cable ipc-stats	12.2(33)SCC
cable ipv6 source-verify leasequery-filter downstream	12.2(33)SCF1

Modified Commands

Command	Cisco IOS Software Release
cable event syslog-server	12.2(33)SCA
cable fiber-node	12.3(23)BC
cable filter group	12.2(33)SCA
cable helper-address	12.2(33)SCB
cable helper-address	12.2(33)SCC
cable freq-range	12.2(33)SCE
cable ipv6 source-verify	12.2(33)SCF1

cable enable-trap

To permanently set four CISCO-DOCS-EXT-MIB MIB attributes that enable the sending of a trap when a CM changes between the online and offline states, use the **cable enable-trap** command in cable interface configuration mode. To return to the default settings found in the MIB, which disable the sending of these traps, use the **no** form of this command.

cable enable-trap [**cmonoff-notification** | **cmonoff-interval** *time-in-secs*]

no cable enable-trap [**cmonoff-notification** | **cmonoff-interval**]

Syntax Description

cmonoff-notification	Enables or disables the sending of the notification traps.
cmonoff-interval	Specifies the minimum interval that must pass before sending out a new trap for the same CM.
time-in-secs	Specifies the number of seconds (0 to 86400 seconds). The default value is 600 seconds.

Command Default

The default is to use the MIB defaults, which specify that traps are not to be sent, with an interval value of 600 seconds (10 minutes).

Command Modes

Interface configuration (cable interface only) (config-if)

Command History

Release	Modification
12.0(13)SC	This command was introduced.
12.1(5)EC1	This command was added to the 12.1 EC train and support was added for the Cisco uBR7100 series routers.
12.2(4)BC1	This command was added to the 12.2 BC train and support was added for the Cisco uBR10012 router.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

This command sets four attributes in the CISCO-DOCS-EXT-MIB MIB, so that the new values can be automatically loaded whenever the CMTS router powers on or reloads. To do so, put the appropriate commands in the configuration file and save it to the CMTS router's Flash memory. The CMTS router automatically sets the appropriate MIB values when it processes the configuration file at startup.

These commands affect whether the CM online/offline notification trap (cdxCmtsCmOnOffNotification) is sent, and if so, the minimum interval that must exist between traps that are sent for the same CM undergoing the same state changes. The following describes the relationship between these commands and the attributes in the CISCO-DOCS-EXT-MIB MIB:

- The **cable enable-trap cmonoff-notification** command sets the cdxCmtsCmOnOffTrapEnable attribute to 1 (true), which enables the sending of the CM online and offline traps.

- The **no cable enable-trap cmonoff-notification** command sets the cdxCmtsCmOnOffTrapEnable attribute to 2 (false), which disables the sending of the CM online and offline traps.
- The **cable enable-trap cmonoff-interval** command sets the cdxCmtsCmOnOffTrapInterval attribute to the specified time period (0 to 86400 seconds), which sets the minimum interval that must exist before the CMTS sends out the same trap for the same CM. For example, if the interval is set to the default of 600 seconds, and the same CM goes offline three times and online twice in that time period, only one online trap and one offline trap is sent to the SNMP manager.
- The **no cable enable-trap cmonoff-interval** command sets the cdxCmtsCmOnOffTrapInterval attribute to 0, which means a trap will be sent for every CM online/offline transition.

Note Setting the **cmonoff-interval** option and the cdxCmtsCmOnOffTrapInterval attribute has meaning only if cdxCmtsCmOnOffNotification traps have been previously enabled.

Examples

The following commands enable the sending of CM on or off traps, with a minimum interval of 1200 seconds between traps being sent for the same CM:

```
router(config)# interface c6/0
router(config-if)# cable enable-trap cmonoff-notification
router(config-if)# cable enable-trap cmonoff-interval 1200
router(config-if)# exit
router(config)#
```

The following commands disable the sending of CM on or off traps.

```
router(config)# interface c6/0
router(config-if)# no cable enable-trap cmonoff-notification
router(config-if)# exit
router(config)#
```

Related Commands

Command	Description
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable event priority

To configure the event reporting flags for DOCSIS event messages, which determines how the Cisco CMTS reports these events, use the **cable event priority** command in global configuration mode. To return to the default settings found in the MIB, use the **no** form of this command.

cable event priority {**alert** | **critical** | **debug** | **emergency** | **error** | **informational** | **notice** | **warning**} *flags*

Syntax Description

alert	Sets the event reporting flag for alert system error messages. (Alert messages indicate that some type of system or connection failure has occurred and requires immediate attention.)
critical	Sets the event reporting flag for critical system error messages. (Critical messages indicate that an error occurred which requires immediate attention to avoid system or connection failure.)
debug	Sets the event reporting flag for debug system error messages. (Debug messages appear only when debugging has been enabled.)
emergency	Sets the event reporting flag for emergency system error messages. (Emergency messages indicate that the system has become unusable and requires immediate attention. This problem might also be affecting other parts of the network.)
error	Sets the event reporting flag for error system error messages. (Error messages indicate that an error condition occurred that requires attention to resolve. Failure to address this problem will result in some type of system or connection failure in the near future.)
informational	Sets the event reporting flag for informational system error messages. (Informational messages might or might not be significant to the system administrators.)
notice	Sets the event reporting flag for notice system error messages. (Notice messages indicate that a situation occurred that is normal but is significant enough that system administrators might want to notice.)
warning	Sets the event reporting flag for warning system error messages. (Warning messages indicate that a condition occurred that indicates attention is needed in near future to avoid potential problems. Failure to address this problem could result in some type of system or connection failure later on.)
flags	Sets the event reporting flags value, in hex, which specifies how this particular type of event message should be reported. The valid range is 0x0 through 0xF0, which is a bitmask specifying the types of reporting that should be done. See the Usage Guidelines for details.

Command Default

The defaults are configured as per the DOCSIS 1.1 Operations Support System Interface (OSSI) Specification:

- Emergency and alert messages = (0x10) (reported to the local volatile log)
- Critical, error, warning, and notice = (0x70) (reported to the local volatile log, and forwarded as traps and to the SYSLOG server)
- Information and debug = 0x0 (not reported)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)BC1	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

The DOCSIS 1.1 specifications require the CMTS to generate a set of messages for DOCSIS-specific events. These messages can be assigned one of eight priority levels, ranging from emergency (the highest level) to debug (the lowest level), and the CMTS can be configured to log each level of messages differently.

The Cisco CMTS supports the following types of logging, as defined by the DOCS-CABLE-DEVICE-MIB MIB (RFC 2669):

- none (0x0) = DOCSIS messages are not reported. (The corresponding Cisco IOS event messages, however, continue to be logged.)
- local-volatile (0x10) = DOCSIS messages are saved in a local log on the CMTS. This log can be limited in size and can automatically discard previous messages to make room for incoming messages.
- syslog (0x20) = DOCSIS messages are sent to a SYSLOG server (if one has been configured, using the **cable event syslog-server** command).
- traps (0x40) = DOCSIS messages are sent as SNMP traps to one or more SNMP managers.

These values can be added together to specify that the CMTS should report an event in more than one way. For example, a value of 0x70 specifies that the CMTS should record the event in its local volatile log, and also send it both as a trap and as a SYSLOG message.

Note If event messages are configured for traps or syslog reporting, they must also be configured for either local volatile or local non-volatile reporting. This means that values 0x20 (syslog-only), 0x40 (trap-only), and 0x60 (syslog and trap only) are not supported.

Use the **cable event priority** command to set the reporting flags for each type of event. This also configures the appropriate instance of the docsDevEvReporting attribute DOCS-CABLE-DEVICE-MIB MIB (RFC 2669) with the same value.

Note This command affects only the DOCSIS event messages, and does not affect how the Cisco IOS software handles event messages. If SYSLOG traps are enabled on the Cisco CMTS (using the **snmp-server enable traps syslog** command), they continue to be sent, regardless of the **cable event priority** configuration.

Examples

The following commands configure the Cisco CMTS so that it reports all emergency, alert, and critical messages as SNMP traps and SYSLOG messages, as well as logging it in the local volatile log:

```
Router# configure terminal
```

```
Router(config)# cable event priority alert 0x70
Router(config)# cable event priority critical 0x70
Router(config)# cable event priority emergency 0x70
```

The following commands configure the Cisco CMTS so that it reports the lowest priority messages only to the local volatile log and SYSLOG server:

```
Router# configure terminal
Router(config)# cable event priority debug 0x30
Router(config)# cable event priority informational 0x30
Router(config)# cable event priority notice 0x30
```

Related Commands

Command	Description
cable event syslog-server	Enables logging of DOCSIS event messages to a SYSLOG server.
cable event throttle-adminStatus	Configures how the Cisco CMTS throttles the SNMP traps and SYSLOG messages it generates for DOCSIS event messages.
cable event throttle-interval	Specifies the throttle interval, which helps control how often the Cisco CMTS generates SNMP traps and SYSLOG messages for DOCSIS event messages.
cable event throttle-threshold	Sets the maximum number of SNMP traps and SYSLOG messages that the Cisco CMTS can generate for DOCSIS event messages during the throttle interval.
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable event syslog-server

To enabling logging of DOCSIS event messages to a SYSLOG server, use the **cable event syslog-server** command in global configuration mode. To disable the logging of a DOCSIS syslog server, use the **no** form of this command.

cable event syslog-server *ip-address*

no cable event syslog-server

Syntax Description

ip-address	Specifies the IPv4 or IPv6 address for the DOCSIS SYSLOG server, which is the docsDevEvSyslog attribute in the DOCS-CABLE-DEVICE-MIB (RFC 2669). If the IP address is 0.0.0.0 or 0:0:0:0::0, SYSLOG service is disabled for DOCSIS events.

Command Default

0.0.0.0 or 0:0:0:0::0 (No DOCSIS SYSLOG server is defined.)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)BC1	This command was introduced.
12.2(33)SCA	This command was modified in Cisco IOS Release 12.2(33)SCA to support IPv6 addresses. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

The DOCSIS 1.1 specifications require the CMTS router to generate a set of messages for DOCSIS-specific events. Use the **cable event syslog-server** command to enable DOCSIS SYSLOG services and to set the IP address for the DOCSIS SYSLOG server (which is the docsDevEvSyslog attribute in the DOCS-CABLE-DEVICE-MIB).

You can also configure the server's IP address by using SNMP commands to set the docsDevEvSyslog attribute directly. Setting the docsDevEvSyslog attribute also creates a matching **cable event syslog-server** command in the router's configuration.

When you specify the IP address for a DOCSIS SYSLOG server, either by using the **cable event syslog-server** command or by setting the docsDevEvSyslog attribute, the Cisco CMTS router begins generating event messages that conform to the DOCSIS 1.1 specifications. This format is similar to but not identical to the format that is used by the Cisco IOS software. For example, the following message is in the typical Cisco IOS software format:

```
%UBR7200-4-DCC_ACK_REJ_MSG_SYNTAX_ERROR: DCC-ACK rejected message syntax error
```

The same error message appears as follows when using the DOCSIS 1.1 format:

```
<133>CMTS[DOCSIS]:<67040500> DCC-ACK rejected message syntax error
```

To disable the sending of events to the DOCSIS SYSLOG server, you can use the **no cable event syslog-server** command, or you can specify an IP address of 0.0.0.0 (**cable event syslog-server 0.0.0.0**). Both commands set the docsDevEvSyslog attribute to 0.0.0.0 and disable DOCSIS SYSLOG service. This does not, however, disable the Cisco IOS SYSLOG server (if one has been configured using the **logging** *ip-address* command).

Note You can use the same SYSLOG server for both Cisco IOS event messages and for DOCSIS-style event messages, but it might be more convenient to use separate servers for the two different message formats. Use the **logging** *ip-address* command in global configuration mode to set the IP address for the Cisco IOS SYSLOG server. The DOCSIS SYSLOG server collects only event messages for DOCSIS events, using the DOCSIS format, while the Cisco IOS server collects all event messages (including DOCSIS events), but using the standard Cisco IOS message format.

Tip For more information about DOCSIS SYSLOG services and event messages, see Section 4.4.2.2.2, SYSLOG Message Format, in the DOCSIS 1.1 Operations Support System Interface (OSSI) Specification (SP-OSSIv1.1-I06-020830). For more information about all cable-related event messages that can be generated on a Cisco CMTS router, see the Cisco CMTS System Messages guide.

Examples

The following command sets the docsDevEvSyslog attribute with an IPv4 address of 192.168.100.137:

```
cable event syslog-server 192.168.100.137
```

The following commands specifies different SYSLOG servers. The server at IPv4 address 192.168.100.137 receives the DOCSIS-style event messages, and the server at IPv4 address 192.168.100.138 receives the Cisco IOS style messages.

```
cable event syslog-server 192.168.100.137
logging 192.168.100.138
```

The following command sets the docsDevEvSyslog attribute to IPv4 address 0.0.0.0, which disables DOCSIS SYSLOG services:

```
no cable event syslog-server
```

Note You can also disable DOCSIS SYSLOG services with the **cable event syslog-server 0.0.0.0** command.

The following command specifies a DOCSIS SYSLOG server with an IPv6 address:

```
cable event syslog-server 2001:0DB8:0:ABCD::1
```

Related Commands

Command	Description
cable event priority	Configures the event reporting flags for DOCSIS event messages, which determines how the Cisco CMTS router reports these events.
cable event throttle-adminStatus	Configures how the Cisco CMTS router throttles the SNMP traps and SYSLOG messages it generates for DOCSIS event messages.

Command	Description
cable event throttle-interval	Specifies the throttle interval, which helps control how often the Cisco CMTS router generates SNMP traps and SYSLOG messages for DOCSIS event messages.
cable event throttle-threshold	Sets the maximum number of SNMP traps and SYSLOG messages that the Cisco CMTS router can generate for DOCSIS event messages during the throttle interval.
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable event throttle-adminStatus

To configure how the Cisco CMTS router throttles the SNMP traps and syslog messages it generates for DOCSIS event messages, use the **cable event throttle-adminStatus** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

cable event throttle-adminStatus {**inhibited** | **maintainBelowThreshold** | **stopAtThreshold** | **unconstrained**}

no cable event throttle-adminStatus

Syntax Description

inhibited	All SNMP traps and syslog messages for DOCSIS event messages are suppressed.
maintainBelowThreshold	Throttling is performed, so that SNMP traps and syslog messages are suppressed if they would otherwise exceed the throttle threshold. The Cisco CMTS resumes generating traps and messages at the start of the next throttle interval.
stopAtThreshold	Throttling is performed, so that the Cisco CMTS stops generating all SNMP traps and syslog messages if they would exceed the throttle threshold. The Cisco CMTS does not resume generating traps and messages until directed to do so by repeating this command.
unconstrained	SNMP traps and syslog messages for DOCSIS event messages are not throttled.

Command Default

unconstrained (no throttling of traps and messages is done)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)BC1	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

This command sets the value of the docsDevEvThrottleAdminStatus attribute in the DOCS-CABLE-DEVICE-MIB MIB (RFC 2669), which controls whether the Cisco CMTS should throttle SNMP traps and syslog messages that are generated for DOCSIS event messages.

The DOCS-CABLE-DEVICE-MIB MIB supports the following threshold configurations:

- inhibited—The Cisco CMTS does not generate any SNMP traps or syslog messages for DOCSIS events.

- maintainBelowThreshold—Throttling is performed, and SNMP traps and syslog messages are suppressed if they would exceed the throttle threshold (as set by the **cable event throttle-interval** and **cable event throttle-threshold** commands). The Cisco CMTS resumes generating traps and messages at the start of the next throttle interval.
- stopAtThreshold—Throttling is performed, and the Cisco CMTS stops generating all SNMP traps and syslog messages when they exceed the throttle threshold. The Cisco CMTS does not resume generating traps and messages until the threshold state is reset. This can be done by repeating the **cable event throttle-adminStatus** command, or by setting the docsDevEvThrottleAdminStatus attribute in the DOCS-CABLE-DEVICE-MIB MIB.
- unconstrained—All SNMP traps and syslog messages are transmitted without any throttling.

Tip For more information about DOCSIS syslog services and event messages, see Section 4.4.2.2.2, syslog Message Format, in the DOCSIS 1.1 Operations Support System Interface (OSSI) Specification (SP-OSSIv1.1-I06-020830). For more information about all cable-related event messages that can be generated on the Cisco CMTS router, see the Cisco CMTS Error Message manual.

Examples

The following commands configure the Cisco CMTS router to throttle SNMP traps and syslog messages according to the specified throttle interval and threshold:

```
Router# configure terminal
Router(config)# cable event throttle-interval 90
Router(config)# cable event throttle-threshold 30
Router(config)# cable event throttle adminStatus maintainBelowThreshold
```

The following commands configure the Cisco CMTS router for the default behavior, so that it does not throttle SNMP traps and syslog messages. The configured throttle interval and threshold are ignored.

```
Router# configure terminal
Router(config)# cable event throttle adminStatus unconstrained
```

Related Commands

Command	Description
cable event priority	Configures the event reporting flags for DOCSIS event messages, which determines how the Cisco CMTS reports these events.
cable event syslog-server	Enables logging of DOCSIS event messages to a syslog server.
cable event throttle-interval	Specifies the throttle interval, which helps control how often the Cisco CMTS generates SNMP traps and syslog messages for DOCSIS event messages.
cable event throttle-threshold	Sets the maximum number of SNMP traps and syslog messages that the Cisco CMTS can generate for DOCSIS event messages during the throttle interval.
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable event throttle-interval

To specify the throttle interval, which controls how often the Cisco CMTS router generates SNMP traps and syslog messages for DOCSIS event messages, use the **cable event throttle-interval** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

cable event throttle-interval *seconds*

no cable event throttle-interval

Syntax Description

seconds	Length of the throttle interval, in seconds. The valid range is 0 to 2147483647 seconds, with a default of 60 seconds.

Command Default

60 seconds (1 minute)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)BC1	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

The DOCSIS 1.1 specifications require the CMTS to generate a set of messages for DOCSIS-specific events. In certain situations, such as a power outage that causes a mass reregistration of cable modems, this can generate such a large volume of event messages that it can impact system performance.

To avoid this possibility, use the **cable event throttle-interval** command, together with the **cable event throttle-threshold** command, to specify the maximum number of SNMP traps or syslog events that the Cisco CMTS can generate for DOCSIS events over a specific interval:

- **cable event throttle-interval**—Specifies the length of the throttle interval.
- **cable event throttle-threshold**—Specifies the maximum number of SNMP traps and syslog events that the Cisco CMTS can generate during that period.

The threshold value counts DOCSIS events, not SNMP traps or syslog messages. If a DOCSIS event generates both an SNMP trap and a syslog message, the Cisco CMTS counts it as only one event.

Note The **cable event throttle-interval** and **cable event throttle-threshold** commands do not have any effect unless the **cable event throttle-adminStatus** has been configured to allow the throttling of DOCSIS event messages.

Tip For more information about DOCSIS syslog services and event messages, see Section 4.4.2.2.2, syslog Message Format, in the DOCSIS 1.1 Operations Support System Interface (OSSI) Specification (SP-OSSIv1.1-I06-020830). For more information about all cable-related event messages that can be generated on the Cisco CMTS router, see the Cisco CMTS Error Message manual.

Examples

The following commands configure the Cisco CMTS router so that it can generate a maximum number of 30 SNMP traps and syslog messages for DOCSIS events over a 90-second period:

```
Router# configure terminal
Router(config)# cable event throttle-interval 90
Router(config)# cable event throttle-threshold 30
```

Related Commands

Command	Description
cable event priority	Configures the event reporting flags for DOCSIS event messages, which determines how the Cisco CMTS reports these events.
cable event syslog-server	Enables logging of DOCSIS event messages to a syslog server.
cable event throttle-adminStatus	Configures how the Cisco CMTS throttles the SNMP traps and syslog messages it generates for DOCSIS event messages.
cable event throttle-threshold	Sets the maximum number of SNMP traps and syslog messages that the Cisco CMTS can generate for DOCSIS event messages during the throttle interval.
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable event throttle-threshold

To set the maximum number of SNMP traps and syslog messages that the Cisco CMTS router can generate for DOCSIS event messages during the throttle interval, use the **cable event throttle-threshold** command in global configuration mode. To restore the default number, use the **no** form of this command.

cable event throttle-threshold *number*

no cable event throttle-threshold

Syntax Description

number	Maximum allowable number of DOCSIS events for which the Cisco CMTS can generate SNMP traps and syslog messages during the throttle period. The valid range is 0 to 2147483647, with a default of 10.

Command Default

The default maximum is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)BC1	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

The DOCSIS 1.1 specifications require the CMTS to generate a set of messages for DOCSIS-specific events. In certain situations, such as a power outage that causes a mass reregistration of cable modems, this can generate such a large volume of event messages that it can impact system performance.

To avoid this possibility, use the **cable event throttle-threshold** command, together with the **cable event throttle-interval** command, to specify the maximum number of SNMP traps or syslog events that the Cisco CMTS can generate for DOCSIS events over a specific interval:

- **cable event throttle-interval**—Specifies the length of the throttle interval.
- **cable event throttle-threshold**—Specifies the maximum number of SNMP traps and syslog events that the Cisco CMTS can generate during that period.

The threshold value counts DOCSIS events, not SNMP traps or syslog messages. If a DOCSIS event generates both an SNMP trap and a syslog message, the Cisco CMTS counts it as only one event.

Note The **cable event throttle-interval** and **cable event throttle-threshold** commands do not have any effect unless the **cable event throttle-adminStatus** has been configured to allow the throttling of DOCSIS event messages.

Tip For more information about DOCSIS syslog services and event messages, see Section 4.4.2.2.2, syslog Message Format, in the DOCSIS 1.1 Operations Support System Interface (OSSI) Specification (SP-OSSIv1.1-I06-020830). For more information about all cable-related event messages that can be generated on the Cisco CMTS router, see the Cisco CMTS Error Message manual.

Examples

The following commands configure the Cisco CMTS router so that it can generate a maximum number of 25 SNMP traps and syslog messages for DOCSIS events over a two-minute period:

```
Router# configure terminal
Router(config)# cable event throttle-interval 120
Router(config)# cable event throttle-threshold 25
```

Related Commands

Command	Description
cable event priority	Configures the event reporting flags for DOCSIS event messages, which determines how the Cisco CMTS reports these events.
cable event syslog-server	Enables logging of DOCSIS event messages to a syslog server.
cable event throttle-adminStatus	Configures how the Cisco CMTS throttles the SNMP traps and syslog messages it generates for DOCSIS event messages.
cable event throttle-interval	Specifies the throttle interval, which helps control how often the Cisco CMTS generates SNMP traps and syslog messages for DOCSIS event messages.
snmp-server enable traps cable	Enables traps for cable-related events.
snmp-server enable traps docsis-cmts	Enables traps for DOCSIS-related MAC-layer events.

cable fiber-node

To enter cable fiber-node configuration mode to configure a fiber node, use the **cable fiber-node** command in global configuration mode. To remove a fiber node configuration, use the **no** form of this command.

cable fiber-node *fiber-node-id*

no cable fiber-node *fiber-node-id*

Syntax Description

fiber-node-id	Specifies a unique numerical ID for the fiber node. Valid values are 1 to 256.

Command Default

The command mode is unchanged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
12.3(23)BC	This command was updated to allow an RF channel from the SPA or a Cisco uBR10-MC5X20 downstream channel can serve as a primary channel in a fiber node.

Usage Guidelines

The **cable fiber-node** command allows the multiple service operator (MSO) or service provider to configure the CMTS to be more intelligent by making Cisco IOS aware of how the cable plant is wired. The downstream channels of the cable plant must be accurately configured in the CMTS fiber nodes. This allows the CMTS to accurately signal the wideband modems on which wideband channels are available to the modem.

In a cable network, a cable modem is physically connected to only one fiber node. Fiber node software configuration mirrors the physical topology of the cable network. When configuring fiber nodes with Cisco IOS CLI commands, a fiber node is a software mechanism to define the following:

- The set of downstream RF channels that will flow into the fiber node
- At least one primary downstream channel

Note In Cisco IOS Releases 12.3(21)BC and 12.3(21a)BC3, this is a traditional DOCSIS downstream channel for the fiber node. Beginning in Cisco IOS Release 12.3(23)BC, either an RF channel from the SPA or a Cisco uBR10-MC5X20 downstream channel can serve as a primary channel in a fiber node.

- The set of upstream channel ports on the cable interface line card that are connected to the fiber node and available as upstream channels

Use the **cable fiber-node** command to enter cable fiber-node configuration mode so that you can configure a fiber node.

For a wideband channel to work correctly, each fiber node must be configured as follows:

1. Use the **cable fiber-node** command to create the fiber node and to enter cable fiber-node configuration mode.
2. Use the **downstream** command to associate the fiber node with one or more primary downstream channels (traditional DOCSIS downstream channels).

   Note Beginning in Cisco IOS Release 12.3(23)BC, if the primary downstream channel for this fiber node is assigned from a SPA RF downstream channel, then this command is not required.

3. Use the **upstream** command to specify the upstream channel ports for a fiber node.
4. Use the **downstream modular-cable rf-channel** command to make one or more SPA RF channels available for the fiber node.
5. Optionally, use the **description** (**cable fiber-node**) command to specify a description for the fiber node.

For each fiber node, a traditional DOCSIS downstream channel on the Cisco uBR10-MC5X20 cable interface line card is used to carry MAC management and signaling messages, and the associated traditional DOCSIS upstream channel is used for return data traffic and signaling. The traditional DOCSIS downstream channel used in this way is called the *primary downstream channel*. Beginning in Cisco IOS Release 12.3(23)BC, either an RF channel from the SPA or a Cisco uBR10-MC5X20 downstream channel can serve as a primary channel in a fiber node. If the fiber node does not have a Cisco uBR10-MC5X20 downstream channel, then make sure that at least one of the SPA RF channels specified in the **downstream modular-cable rf-channel** command is a primary-capable downstream channel.

Each wideband channel must be associated with at least one primary downstream channel and can be associated with multiple primary downstream channels. A wideband channel and its associated primary downstream channels must be belong to the same virtual bundle interface.

The maximum number of cable fiber nodes that can be configured is limited to 256 for each CMTS.

Examples

The following example shows how to enter configuration mode for fiber node 5.

Cisco IOS Release 12.3(21)BC

```
Router# configure terminal
Router(config)# cable fiber-node 5
Router(config-fiber-node)#
downstream Cable 6/0/0
downstream Modular-Cable 1/0/0 rf-channel 0-1
upstream cable 5/0 connector 0
```

Cisco IOS Release 12.3(23)BC

```
Router# configure terminal
Router# cable fiber-node 5
Router(config-fiber-node)#
downstream Modular-Cable 1/0/0 rf-channel 0-3
upstream cable 5/0 connector 0
```

Related Commands

Command	Description
description (cable fiber-node)	Specifies a description for a fiber node.
downstream cable	Assigns a primary downstream channel for a fiber node.
downstream modular-cable rf-channel	Specifies the RF channels that are available for wideband channels on a fiber node.
upstream cable connector	Specifies the upstream channel ports for a fiber node.

cable filter group

To create, configure, and activate a DOCSIS 1.1 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. To delete a filter group or to reset a particular option to its default value, use the **no** form of this command.

cable filter group *group-id* **index** *index-num* [*option option-value*]

no cable filter group *group-id* **index** *index-num* [*option option-value*]

Syntax Description

group-id	Specifies a unique group ID for this filter group. The valid range is 1 to 254. 255 is reserved for use by the CMTS router.
index-num	Specifies a unique index for this particular filter. The valid range is 1 to 128 on a uBR7200 series router and 1 to 255 on a uBR10012 router.
Specify one of the following options and option-values:	
dest-ip *ip-address*	(Optional) Specifies the destination IP address that should be matched. The default IP address is 0.0.0.0. (IPv4 filters only)
dest-mac-addr *mac-address*	(Optional) Specifies the destination MAC address that should be matched.
dest-mac-mask *mask*	(Optional) Specifies the mask for the destination MAC address that should be matched.
dest-mask *mask*	(Optional) Specifies the mask for the destination address that should be matched. The *mask* is ANDed with the IP address specified by the **dest-ip** option and compared to the result of ANding the *mask* with the packet's destination IP address. The filter considers it a match if the two values are the same. (IPv4 filters only) **Note** The default mask of 0.0.0.0 matches all IP addresses.
dest-port *port-number*	(Optional) Specifies the TCP/UDP destination port number that should be matched. The valid range is 0 to 65535. The default value matches all TCP/UDP port numbers. (IPv4 and IPv6 filters)
eth-proto-type *ethernet protocol type*	(Optional) Specifies the Ethernet protocol type number that should be matched. The valid range is 0 to 65536.
eth-protocol *ethernet protocol number*	(Optional) Specifies the Ethernet protocol that should be matched. The valid range is 0 to 65536.
ip-proto *proto-type*	(Optional) Specifies the IP protocol type number that should be matched. The valid range is 0 to 256, with a default value of 256 that matches all protocols. (IPv4 and IPv6 filters) Some commonly-used values are: • 1—ICMP, Internet Control Message Protocol. • 2—IGMP, Internet Group Management Protocol. • 4—IP in IP encapsulation. • 6—TCP, Transmission Control Protocol. • 17—UDP, User Datagram Protocol.

ip-tos *tos-mask tos-value*	(Optional) Specifies a type of service (TOS) mask and value to be matched (IPv4 and IPv6 filters): • *tos-mask*—8-bit value expressed in hexadecimal notation. The valid range is 0x00 through 0xFF. • *tos-value*—8-bit value expressed in hexadecimal notation. The valid range is 0x00 through 0xFF. The *tos-mask* is logically ANDed with the *tos-value* and compared to the result of ANDing the *tos-mask* with the packet's actual TOS value. The filter considers it a match if the two values are the same. **Note** The default values for both parameters matches all ToS values.
ip-version	(Optional) Specifies the IP version of the filter: • **ipv4**—Filter is an IP version 4 filter group (default). • **ipv6**—Filter is an IP version 6 filter group.
match-action {**accept** | **drop**}	(Optional) Specifies the action that should be taken for packets that match this filter (IPv4 and IPv6 filters): • **accept**—Packets that match the filter are accepted (default). • **drop**—Packets that match the filter are dropped.
range-dest-port *start-port number end-port number*	(Optional) Specifies the TCP/UDP destination port start range. The valid range is 0 to 65535.
range-ip-tos *mask against TOS start value and end value*	(Optional) Specifies IP TOS byte range settings expressed in hexadecimal notation. The valid range is 0x00 through 0xFF.
range-src-port *start-port number end-port number*	(Optional) Specifies TCP/UDP source port start range. The valid range is 0 to 65535.
range-user-pri *low-priority value high-priority value*	(Optional) Specifies the user priority.The valid range for priority is 0 to 8. The Priority field indicates the frame priority level from 0 (lowest) to 8 (highest), which prioritizes different classes of traffic (such as voice, video and data).
src-ip *ip-address*	(Optional) Specifies the source IP address that should be matched. The default IP address is 0.0.0.0. (IPv4 filters only)
src-mac-addr *mac address*	(Optional) Specifies the source MAC address to be matched.
src-mask *mask*	(Optional) Specifies the mask for the source address that should be matched. The *mask* is ANDed with the IP address specified by the **src-ip** option and compared to the result of ANDing the *mask* with the packet's source IP address. The filter considers it a match if the two values are the same. (IPv4 filters only) **Note** The default mask of 0.0.0.0 matches all IP addresses.
src-port *port-number*	(Optional) Specifies the TCP/UDP source port number that should be matched. The valid range is 0 to 65535. The default value matches all TCP/UDP port numbers. (IPv4 and IPv6 filters)

status {**active** | **inactive**}	(Optional) Enables or disables the filter (IPv4 and IPv6 filters): • **active**—Enables the filter immediately (default). • **inactive** —Disables the filter immediately. **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.
tcp-flags *flags-mask flags-value*	(Optional) Specifies the TCP flag mask and value to be matched (IPv4 and IPv6 filters): • *flags-mask*—8-bit value expressed in hexadecimal notation. The valid range is 0x0 through 0x3F. • *flags-value*—8-bit value expressed in hexadecimal notation. The valid range is 0x0 through 0x3F.
v6-dest-address *ipv6-address*	(Optional) Specifies the IPv6 destination address that should be matched using the format X:X:X:X::X. (IPv6 filters only)
v6-dest-pfxlen *prefix-length*	(Optional) Specifies the length of the network portion of the IPv6 destination address. The valid range is 0 to 128. (IPv6 filters only)
v6-flow-label *flow-label value*	(Optional) Specifies the IPv6 flow label to be used by the source to label packets of a flow. The range is 0 to 1048575. A flow label of zero is used to indicate packets not part of any flow.
v6-src-address *ipv6-address*	(Optional) Specifies the IPv6 source address that should be matched using the format X:X:X:X::X. (IPv6 filters only)
v6-src-pfxlen *prefix-length*	(Optional) Specifies the length of the network portion of the IPv6 source address. The valid range is 0 to 128. (IPv6 filters only)
vlan-id *vlan-id*	(Optional) Specifies the VLAN Identifier to be matched, which is a 12-bit field specfying the VLAN to which the packet belongs.The valid range is 0 to 4094.

Command Default

No filter groups are defined. When a filter group is created, it defaults to accepting all source and destination IP addresses and TCP/UDP ports, all protocol types, and all ToS and TCP flag values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(6)EC1	This command was introduced on the Cisco uBR7100 series and Cisco uBR7200 series routers.
12.2(2)XF, 12.2(4)BC1	This command was supported on the Cisco uBR10012 routers.
12.2(8)BC2	The **status** option was added to allow filter groups to be activated and deactivated without removing the filter group's configuration.
12.2(33)SCA	The **v6-src-address**, **v6-dest-address**, **v6-src-pfxlen**, **v6-dest-pfxlen**, and **ip-version** keyword options were added for support of IPv6 filter groups. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

This command implements DOCSIS 1.1 packet filtering, as defined in the DOCS-SUBMGT-MIB. Each filter group can contain multiple filters, as defined by the different index numbers.

Note The DOCS-SUBMGT-MIB MIB is supported only on Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases. See the description of the docsSubMgtPktFilterTable table in this MIB for further information.

Note Before configuring layer 4 **src-port** and **dest-port** options, configure the IP protocol number using the **ip-proto** option. If a layer 4 IP protocol is not configured, the default value (256) is used and the filter groups configured with multiple filters will fail.

When matching the source or destination addresses, the filter ANDs the mask value with the filter's corresponding IP address. The filter then ANDs the mask with the packet's actual IP address and compares the two values. If they are the same, the filter matches the packet.

For example, if you specify a **src-ip** of 192.168.100.0 and a **src-mask** of 255.255.255.0, the filter matches all packets that have a source IP address in the range of 192.168.100.0 through 192.168.100.255. Use a mask value of 0.0.0.0 (default) to match all IP addresses. Use a mask value of 255.255.255.255 to match one specific IP address.

Similarly, when comparing TOS values, the filter ANDs the *tos-mask* parameter with the *tos-value* parameter and compares it to the result of ANDing the *tos-mask* parameter with the packet's actual TOS value. If the two values are the same, the filter matches the packet.

Note For the filter group to work for CMs, a CM must re-register after the CMTS router is configured.

Cable Subscriber Management Guidelines

Cable subscriber management is a DOCSIS 1.1 specification, whose functionality 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)

There are certain CMTS configuration requirements if the CM DOCSIS 1.1 configuration file is not used to activate cable subscriber management for the CPE. Specifically, if the docsSubMgtCpeActive object is not provisioned using TLVs 35, 36, and 37 in the DOCSIS 1.1 CM configuration file, then the object uses the docsSubMgtCpeActiveDefault object setting, which is false. This means that cable subscriber management functionality is disabled.

Therefore, if you do not provision TLVs 35, 36, and 37, then you must activate the functionality by specifying the **cable submgmt default active** global configuration command on the CMTS router.

Note Since 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 CMTS router and activate it by using the **cable submgmt default active** global configuration command.

IPv6 Cable Filter Group Guidelines

Note When parallel eXpress forwarding (PXF) is configured on the Cisco ubR10012 router, either the interface ACL (**ip access-list** command) or the **cable filter group** commands can be used to filter the packets.

Consider the following restrictions and guidelines when configuring IPv6 cable filter groups:

- Chained IPv6 headers are not supported.
- 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**.

Examples

The following example shows configuration of an IPv4 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:

```
configure terminal
cable filter group 10 index 10 src-ip 10.7.7.7
cable filter group 10 index 10 src-mask 255.255.0.0
cable filter group 10 index 10 dest-ip 10.8.8.8
cable filter group 10 index 10 dest-mask 255.255.0.0
cable filter group 10 index 10 ip-proto 256
cable filter group 10 index 10 src-port 2000
cable filter group 10 index 10 dest-port 3000
cable filter group 10 index 10 tcp-flags 0 0
cable filter group 10 index 10 match-action drop
```

IPv6 Example

The following example shows the configuration of an IPv6 filter group that drops traffic from a specific IPv6 host (with source address 2001:33::20B:BFFF:FEA9:741F/128) behind a cable router to an IPv6 host on the network (with destination address 2001:1::224/128):

```
configure terminal
!
! Specify the filter group criteria using ID 254
!
cable filter group 254 index 128 v6-src-address 2001:33::20B:BFFF:FEA9:741F
cable filter group 254 index 128 v6-src-pfxlen 128
cable filter group 254 index 128 v6-dest-address 2001:1::224
cable filter group 254 index 128 v6-dest-pfxlen 128
!
! Specify that the filter group is IPv6
!
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
```

Related Commands

Command	Description
show cable filter	Displays the DOCSIS 1.1 filter groups that are currently defined.
cable submgmt default	Sets the default values for attributes in the Subscriber Management MIB (DOCS-SUBMGT-MIB), and enables the Cisco Static CPE Override feature on the Cisco CMTS.

cable flap-list aging

To specify the number of days to keep a CM in the flap-list table before aging it out of the table, use the **cable flap-list aging** command in global configuration mode. To disable this feature, use the **no** form of this command.

cable flap-list aging *minutes*

no cable flap-list aging

Syntax Description

minutes	Specifies how long, in minutes, that a CM remains in the flap list. The valid range is 1 to 86400, with a default of 10080 minutes.

Command Default

The default length of time that a CM is kept in the flap-list table is 10080 minutes (1 week).

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(4)XA, 12.1 T, 12.1 EC	The *days* parameter was removed.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

Flapping refers to the rapid disconnecting and reconnecting of a CM that is having problems holding its connection to the CMTS. A flap list is a table maintained by the Cisco CMTS for every modem (active or not) that is having communication difficulties. The flap list contains modem MAC addresses and logs the time of the most recent activity. You can configure the size and entry thresholds for the flap list.

Examples

The following example shows how to specify that the flap-list table retain 2400 minutes (40 hours) of performance for this CM:

```
Router(config)# cable flap-list aging 2400
```

Related Commands

Command	Description
cable flap-list insertion-time	Sets the insertion time interval that determines whether a CM is placed in the flap list.
cable flap-list miss-threshold	Specifies miss threshold for recording a flap-list event.
cable flap-list power-adjust threshold	Specifies the power-adjust threshold for recording a CM flap-list event.

Command	Description
cable flap-list size	Specifies the maximum number of CMs that can be listed in the flap-list table.
clear cable flap-list	Clears all the entries in the flap-list table.
debug cable flap	Displays information about the operation of the CM flap list that is maintained for the cable interfaces.
ping docsis	Sends a DOCSIS ping to a CM and increments the flap-list counters as appropriate.
show cable flap-list	Displays the current contents of the flap list.

cable flap-list insertion-time

To set the cable flap-list insertion time interval, use the **cable flap-list insertion-time** command in global configuration mode. To disable insertion time, use the **no** form of this command.

cable flap-list insertion-time *seconds*

no **cable flap-list insertion-time**

Syntax Description

seconds	Insertion time interval in seconds. Valid values are from 60 to 86,400 seconds. The default value is 180 seconds (3 minutes).

Command Default

The default insertion time interval is 180 seconds (3 minutes).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1 T	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

This command controls the operation of a flapping modem detector. When a CM makes two or more initial Ranging Requests (also known as insertion or reinsertion requests) within the period of time defined by this command, the CM is placed in the flap list. A CM is not put into the flap list if the time between its two consecutive initial Ranging Requests is greater than the insertion time interval.

For example, if the CMTS is configured for the default insertion time of three minutes, and if the CM reinserts itself four minutes after its last insertion, the CM is not placed in the flap list. However, if the CM reinserts itself two minutes after its last insertion, the CM is placed in the flap list.

Also, a CM is put into the flap list only once for each insertion time interval, even if the CM reinserts itself multiple times. For example, if the CMTS is set for the default insertion time interval of 3 minutes, and the CM reinserts itself three times within that period, the flap list will show that the CM has flapped once. If the CM reinserts itself three times within the first 3 minute period and three more times within the next 3 minute period, the flap list will show that the CM has flapped twice.

Examples

The following example shows how to set the insertion time interval to 62 seconds:

```
Router(config)# cable flap-list insertion-time 62
```

Related Commands

Command	Description
cable flap-list aging	Specifies the number of days to keep a CM in the flap-list table before aging it out of the table.
cable flap-list miss-threshold	Specifies miss threshold for recording a flap-list event.
cable flap-list power-adjust threshold	Specifies the power-adjust threshold for recording a CM flap-list event.
cable flap-list size	Specifies the maximum number of CMs that can be listed in the flap-list table.
clear cable flap-list	Clears all the entries in the flap-list table.
debug cable flap	Displays information about the operation of the CM flap list that is maintained for the cable interfaces.
ping docsis	Sends a DOCSIS ping to a CM and increments the flap-list counters as appropriate.
show cable flap-list	Displays the current contents of the flap list.

cable flap-list miss-threshold

To set the miss threshold for recording a flap-list event, use the **cable flap-list miss-threshold** command in global configuration mode. To disable this function, use the **no** form of this command.

cable flap-list miss-threshold *misses*

no **cable flap-list miss-threshold**

Syntax Description

misses	Specifies the number of consecutive MAC-layer keepalive (Station Maintenance) that can be missed before a CM is placed in the flap list. The valid range is 1 to 12, with a default of 6.

Command Default

The default number of station maintenance messages that can be missed is 6.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1 T	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

In a DOCSIS network, the CMTS regularly sends out MAC-layer keepalive messages, known as station maintenance messages, to each CM that is online. If a CM does not respond to a station maintenance message, the CMTS repeats sending these messages either until the CM responds or the CMTS reaches the maximum allowable number of messages that can be sent.

The **cable flap-list miss-threshold** command specifies how many consecutive station maintenance messages can be missed before the cable modem is placed in the flap list. A miss occurs when a CM does not reply to a station maintenance message.

Note Station maintenance messages are occasionally lost due to noise or congestion in a typical DOCSIS network, with a loss rate of approximately 8 percent considered nominal. A higher miss rate can indicate RF plant problems, such as intermittent upstream problems, fiber laser clipping, or common-path distortion.

Examples

The following example shows how to set the miss threshold to 5:

```
Router(config)# cable flap-list miss-threshold 5
```

Related Commands

Command	Description
cable flap-list aging	Specifies the number of days to keep a CM in the flap-list table before aging it out of the table.
cable flap-list insertion-time	Sets the insertion time interval that determines whether a CM is placed in the flap list.
cable flap-list power-adjust threshold	Specifies the power-adjust threshold for recording a CM flap-list event.
cable flap-list size	Specifies the maximum number of CMs that can be listed in the flap-list table.
clear cable flap-list	Clears all the entries in the flap-list table.
debug cable flap	Displays information about the operation of the CM flap list that is maintained for the cable interfaces.
ping docsis	Sends a DOCSIS ping to a CM and increments the flap-list counters as appropriate.
show cable flap-list	Displays the current contents of the flap list.

cable flap-list power-adjust threshold

To specify the power-adjust threshold for recording a flap-list event, use the **cable flap-list power-adjust threshold** command in global configuration mode. To disable power-adjust thresholds, use the **no** form of this command.

cable flap-list power-adjust threshold *dB*

no cable flap-list power-adjust threshold

Syntax Description

dB	Specifies the minimum power adjustment, in decibels, that results in a flap-list event. Valid values are from 1 to 10 dB.

Command Default

The default minimum power adjustment threshold is 2 dB.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1 T	This command was introduced.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

This command controls the operation of a flapping modem detector. When the power adjustment of a CM exceeds the configured threshold value, the modem is placed in the flap list.

Note A power adjustment threshold of less than 2 dB might cause excessive flap-list event recording. Cisco recommends setting this threshold value to 3 dB or higher.

Note For underground HFC networks with 4 amplifier cascade length, a typical threshold value should be 3 dB. For overhead HFC networks with 4 amplifier cascade length, a typical threshold value should be 4 dB. Longer coaxial cascades without return path thermal gain control and sites with extreme daily temperatures will have larger threshold ranges.

Examples

The following example shows the power-adjust threshold being set to 5 dB:

```
Router(config)# cable flap-list power-adjust threshold 5
```

Related Commands

Command	Description
cable flap-list aging	Specifies the number of days to keep a CM in the flap-list table before aging it out of the table.
cable flap-list insertion-time	Sets the insertion time interval that determines whether a CM is placed in the flap list.
cable flap-list miss-threshold	Specifies miss threshold for recording a flap-list event.
cable flap-list size	Specifies the maximum number of CMs that can be listed in the flap-list table.
clear cable flap-list	Clears all the entries in the flap-list table.
debug cable flap	Displays information about the operation of the CM flap list that is maintained for the cable interfaces.
ping docsis	Sends a DOCSIS ping to a CM and increments the flap-list counters as appropriate.
show cable flap-list	Displays the current contents of the flap list.

cable flap-list size

To specify the maximum number of CMs that can be displayed from the flap-list table, use the **cable flap-list size** command in global configuration mode. To reset it to the default flap-list table size, use the **no** form of this command.

cable flap-list size *number*

no cable flap-list size

Syntax Description

number	Maximum number of CMs to be displayed. Valid values are from 1 to 8191 depending on the type of line cards, with a default of 100 CMs.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1 T	This command was introduced.

Usage Guidelines

- The flap-list size is determined by the architecture of the CMTS and the cable line cards. Previously, the cable flap-list tables were stored on the Route Processors and Performance Routing Engine (PRE) modules.
- The legacy non-distributed cable line cards, Cisco uBR-MC16C/MC16E/MC16S line card and Cisco uBR-MC28C/MC28E line card did not store the flap-list tables in the line cards.
- The distributed line cards are designed such that they store the flap-list tables on the line cards. For a CMTS using distributed line cards, the flap-list size is the maximum size per line card.
- The distributed line cards supported on a Cisco uBR7200 router are Cisco uBR-MC28U/X and Cisco uBR-16U/16X.
- The distributed line cards supported on a Cisco uBR10012 router are Cisco uBR10-MC5X20S/U/H.
- You can calculate the flap list sizes using the following formulas:
  - For a Cisco uBR10012 router without line card high availability (LC-HA)—8191 * (Number of cable line cards)
  - For a Cisco uBR10012 router with line card high availability (LC-HA)—8191 * (Number of cable line cards - 1)
  - For a Cisco uBR72VXR router using legacy and distributed line cards—8191 * (1 + Number of distributed cable line cards)
- The flap-list tables sizes are as follows:
  - A fully loaded Cisco uBR10012 router

    With distributed line cards and no LC-HA configured—8191 * 8 = 65528 CMs.

With distributed line cards and LC-HA configured—8191 * (8-1) = 57337 CMs.

Note Legacy line cards behave as the distributed line cards on a Cisco uBR10012 router. Thus, the flap-list sizes are same as for distributed line cards.

- A fully loaded Cisco uBR7246VXR router

  With distributed line cards— 8191 * 6 = 49146 CMs.

  With legacy line cards—8191 * (1+0) = 8191 CMs.

  With legacy and distributed line cards— 8191 * (1 + no of the distributed line cards) CMs.

Examples

The following example shows how to display a maximum of 200 flap-list entries:

```
Router#configure terminal
Router(config)#cable flap-list size 200
Router(config)#
```

Related Commands

Command	Description
cable flap-list aging	Specifies the number of days to keep a CM in the flap-list table before aging it out of the table.
cable flap-list insertion-time	Sets the insertion time interval that determines whether a CM is placed in the flap list.
cable flap-list miss-threshold	Specifies miss threshold for recording a flap-list event.
cable flap-list power-adjust threshold	Specifies the power-adjust threshold for recording a CM flap-list event.
clear cable flap-list	Clears all the entries in the flap-list table.
debug cable flap	Displays information about the operation of the CM flap list that is maintained for the cable interfaces.
ping docsis	Sends a DOCSIS ping to a CM and increments the flap-list counters as appropriate.
show cable flap-list	Displays the current contents of the flap list.

cable freq-range

To configure the Cisco CMTS router for the range of frequencies that are acceptable on upstreams, use the **cable freq-range** command in global configuration mode. To restore the default value (which is based on the cable interface and on the Annex A/B configuration), use the **no** form of this command.

cable freq-range [**european** | **japanese** | **north-american**]

no cable freq-range

Note The frequency range specified in this command does not apply to upstreams of the Cisco uBR-MC3GX60V cable interface line cards. To specify the upstream frequency for the Cisco uBR-MC3GX60V cable interface line card, use the **cable upstream frequency** command.

Syntax Description

european	Configures the Cisco CMTS router to accept upstream frequency ranges that conform with the EuroDOCSIS specifications (5 MHz to 65 MHz).
japanese	Configures the Cisco CMTS router to accept upstream frequency ranges that conform to the extended range used in Japan (5 MHz to 55 MHz).
north-american	Configures the Cisco CMTS router to accept upstream frequency ranges that conform to the DOCSIS specifications (5 MHz to 42 MHz).

Command Default

no cable freq-range, which defaults to a frequency range based on the Annex configuration:

- Annex A = **european** (EuroDOCSIS, 5 MHz to 65 MHz)—Supported only on cable interfaces that support EuroDOCSIS
- Annex B = **north-american** (DOCSIS, 5 MHz to 55 MHz)—All cable interfaces support the 5 MHz to 42 MHz range. The 42 MHz to 55 MHz range is supported only on certain cable interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

In Cisco IOS Release 12.2(15)BC2 and later, the Cisco CMTS router supports three different modes of operation, depending on the cable interface line cards being used. The range of frequencies that are allowed in each mode are as follows:

- North American DOCSIS (Annex B)—Upstreams use frequencies between 5 MHz and 42 MHz. This range is supported by all cable interface line cards.

- European EuroDOCSIS (Annex A)—Upstreams use frequencies between 5 MHz and 65 MHz.
- Japanese Extended Range (Annex B)—Upstreams use frequencies between 5 MHz and 55 MHz.

To configure the router so that it supports the proper range of upstream frequencies, use the **upstream freq-range** command. After you have configured the router with the **cable freq-range** command, the **cable upstream frequency** and **cable spectrum-group (interface configuration)** commands then accept only frequencies that are in the configured range.

Typically, the **upstream freq-range** command is not needed because the default behavior covers the most common configurations. However, this command can be used in the following situations:

- This command is required to enable EuroDOCSIS operations on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards.
- This command is never needed for the Cisco uBR-MC5X20U card nor for EuroDOCSIS cable interfaces (Cisco uBR-MC16E card, and the Cisco uBR7111E and Cisco uBR7114E routers), because these interfaces default to the EuroDOCSIS range of frequencies. However, if you have previously used this command to restrict the allowable range of frequencies, you must use the **european** option to re-enable the EuroDOCSIS range of frequencies.
- The **north-american** option is usually not needed, because this is the default mode of operations for all DOCSIS cable interfaces. However, this option can be useful on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards when noise exists on the frequencies above 42 MHz. In this situation, using the **north-american** option filters out the higher frequencies and reduces the impact of that noise.
- Similarly, the **japanese** option is not needed on those cable interface cards that support it, because this is the default configuration on those cards. However, if you have previously used the **north-american** option on an interface, you need to use the **japanese** option to re-enable the extended frequency range.
- Even when the **upstream freq-range** command is not needed to enable a frequency range, using it ensures that the **cable upstream frequency** and **cable spectrum-group** commands allow only frequencies that are within the desired range. This can help operators from assigning invalid frequencies to upstreams.

Tip If one or more cable interface line cards that are installed in the chassis do not support the frequency range that you select with this command, the command displays an informational warning message for each of those cable interface cards. Also, 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.

Note This command configures only the range of frequencies that can be configured on an upstream. It does not configure the upstreams for the DOCSIS (Annex B) or EuroDOCSIS (Annex A) modes of operation, which is done using the **cable downstream annex** interface command. (Annex C mode is not supported.) You must configure the downstream for Annex A for EuroDOCSIS operations and Annex B for DOCSIS operations. You can configure certain cable interface cards (such as the Cisco uBR-MC28U) for both the DOCSIS Annex B mode and the EuroDOCSIS frequency range, but this violates the DOCSIS specifications and should not be used on standard DOCSIS networks.

The allowable range for the upstream channel frequency depends on the cable interface line card and Cisco IOS software release being used. See Table 2-11 for the currently supported values.

Table 0-9 Allowable Frequency Range for Cable Interface Line Cards

Frequency Range	Supported Cable Interfaces	Minimum Cisco IOS Releases
5 to 42 MHz	All cable interfaces	All releases supported for the Cisco CMTS
5 to 55 MHz	Cisco uBR-MC16E, Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, Cisco uBR-MC5X20U	Cisco IOS Release 12.2(15)BC2
5 to 65 MHz	Cisco uBR-MC16E, Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, Cisco uBR-MC5X20U, Cisco uBR7111E and Cisco uBR7114E routers	Cisco IOS Release 12.0(13)SC and 12.1(4)EC for Cisco uBR-MC16E Cisco IOS Release 12.1(5)EC1 for Cisco uBR711E and Cisco uBR7114E Cisco IOS Release 12.2(15)BC2 for Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20U

Note The **cable freq-range** command fails if any upstreams or spectrum groups on the router are currently configured for a frequency that is outside the new range being selected. You must reconfigure those upstreams or spectrum groups, using the **cable upstream frequency** or **cable spectrum-group** commands, for lower frequencies, and then repeat the **cable freq-range** command.

Examples

The following example shows how to configure the Cisco CMTS router to support the EuroDOCSIS upstream frequency range of 5 MHz to 65 MHz. The router then displays a list of the cable interface line cards, if any, that do not support this range. After giving this command, the **cable upstream frequency** command shows the valid range of upstream frequencies as being the EuroDOCSIS range:

```
Router# configure terminal
Router(config)# cable freq-range european

Interface Cable3/0 does not support European frequency range
Interface Cable3/1 does not support European frequency range
Interface Cable5/0 does not support European frequency range
Interface Cable5/1 does not support European frequency range

Router(config)# interface cable 6/0 ! This cable interface supports EuroDOCSIS
Router(config-if)# cable upstream 0 frequency ?

  <5000000-65000000>  Return Frequency in HZ

Router(config-if)#
```

The following example shows how to configure the Cisco CMTS router to support the extended Japanese upstream frequency range of 5 MHz to 55 MHz. The router then displays a list of the cable interface line cards, if any, that do not support this range. After giving this command, the **cable upstream frequency** command shows the valid range of upstream frequencies as being the extended frequency range for Japanese networks:

```
Router# configure terminal
Router(config)# cable freq-range japanese

Interface Cable3/0 does not support Japanese frequency  range
```

```
Interface Cable4/0 does not support Japanese frequency  range
Interface Cable5/0 does not support Japanese frequency  range

Router(config)# interface cable 6/0 ! This cable interface supports the Japanese range
Router(config-if)# cable upstream 0 frequency ?

  <5000000-55000000>  Return Frequency in HZ
```

The following example shows how to configure the Cisco CMTS router for its default configuration (DOCSIS upstream frequency range of 5 MHz to 42 MHz). (No warning messages are displayed with this configuration because all cable interface line cards support the basic DOCSIS frequency range.) After giving this command, the **cable upstream frequency** command shows the valid range of upstream frequencies as being the DOCSIS range:

```
Router# configure terminal
Router(config)# cable freq-range north-american
Router(config)# interface cable 3/0
Router(config-if)# cable upstream 0 frequency ?

  <5000000-42000000>  Return Frequency in HZ
```

The following example shows all of the commands that are needed to configure the cable interface and upstream on a Cisco uBR-MC28U/X cable interface line card to support a frequency in the EuroDOCSIS upstream frequency range of 5 MHz to 65 MHz:

```
Router# configure terminal
Router(config)# cable freq-range european
Router(config)# interface 3/0
Router(config-if)# cable downstream annex a
Router(config-if)# cable upstream 0 frequency 62500000
```

The following example shows the **cable freq-range** command failing because an upstream is configured for a frequency that is invalid for the new range. The upstream must be reconfigured before the **cable freq-range** command can be given successfully.

```
Router# configure terminal
Router(config)# cable freq-range japanese

%%Interface Cable 3/0/U0 has invalid frequency (62500000 Hz) for specified range
%%Set upstream frequencies within range prior to changing freq-range

Router(config)# interface 3/0
Router(config-if)# cable upstream 0 frequency 38600000
Router(config-if)# exit
Router(config)# cable freq-range japanese
```

Related Commands

Command	Description
cable downstream annex	Sets the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card.
cable upstream frequency	Configures a fixed frequency of the upstream radio frequency (RF) carrier for an upstream port.

cable helper-address

To specify a destination IP address for User Datagram Protocol (UDP) broadcast Dynamic Host Configuration Protocol (DHCP) packets, use the **cable helper-address** command in cable interface or subinterface configuration mode. To disable this feature, use the **no** form of this command.

cable helper-address *IP-address* [**cable-modem | host | mta | stb**]

no cable helper-address *IP-address* [**cable-modem | host | mta | stb**]

Syntax Description

IP-address	The IP address of a DHCP server to which UDP broadcast packets will be sent.
cable-modem	(Optional) Specifies that only CM UDP broadcasts are forwarded.
host	(Optional) Specifies that only host UDP broadcasts are forwarded.
mta	(Optional) Specifies that only media terminal adapter (MTA) UDP broadcasts are forwarded.
stb	(Optional) Specifies that only set-top box (STB) UDP broadcasts are forwarded.

Command Default

If no options are specified, both CM and host UDP broadcasts are forwarded.

Command Modes

Interface configuration—cable interface only (config-if)

Subinterface configuration—cable interface only (config-subif)

Command History

Release	Modification
12.1 T	This command was introduced.
12.1(3a)EC	This command was modified to add the subinterface support.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.3(33)SCB and the **mta** and **stb** keywords were added.

Usage Guidelines

This command enables CMs and their attached CPE devices (hosts) to use separate DHCP servers, so that CMs and hosts receive their IP addresses from separate address pools. The **cable-modem** keyword specifies that only UDP DHCP broadcasts from CMs are forwarded to that particular destination IP address. The **host** keyword specifies that only UDP broadcasts from hosts (CPE devices) are forwarded to that particular destination IP address.

Note You must specify both the **cable-modem** or **host** options in separate commands, using separate IP addresses, if you decide to use them. If you specify only one option, then the other type of device (cable modem or host) will not be able to connect with a DHCP server. In addition, if you use the **cable-modem** or **host** option with the same IP address that was previously configured with this command, the new configuration overwrites the old configuration.

Note Starting with Cisco IOS Release 12.2(33)SCG, if you use the **cable-modem** or **host** option with the same IP address that was previously configured with this command on the Cisco uBR10012 and Cisco uBR7200 series routers, the new configuration does not overwrite the old configuration. It is configured under a bundle interface.

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.

The **cable helper-address** command is similar to the **ip helper-address** command, but the **cable helper-address** command has been enhanced for cable interfaces and DOCSIS networks to allow separate helper addresses for CMs and hosts. Use only the **cable helper-address** command on cable interfaces, and use the **ip helper-address** command on all non-cable interfaces.

The **cable helper-address** command, as is the case with the **ip helper-address** command, cannot be used on slave interfaces, so these commands are automatically removed from an interface configuration when the interface is configured as a slave interface. Slave interfaces use the IP configuration of the master interface, which includes not only the IP address for the interface itself, but also the helper addresses that have been configured on the master interface.

Tip You can repeat this command to specify any number of helper addresses, but the Cisco IOS software uses only the first 16 valid addresses that are configured on each interface (using either the **cable helper-address** command or the **ip helper-address** command) when forwarding DHCP requests.

Examples

The following example shows how to forward UDP broadcasts from both CMs and CPE devices to the DHCP server at 172.23.66.44:

```
Router(config)# interface cable 1/0
Router(config-if)# cable helper-address 172.23.66.44
Router(config-if)# exit
Router(config)#
```

The following example shows how to forward UDP broadcasts from CMs and CPE devices to separate DHCP servers:

```
Router(config)# interface cable 6/0
Router(config-if)# cable helper-address 172.23.66.143 host
Router(config-if)# cable helper-address 172.23.66.144 cable-modem
Router(config-if)# exit
Router(config)#
```

The following example shows that when you specify the **cable-modem** and **host** options with the same IP address, the second command overwrites the first one:

```
Router(config)# interface cable 3/0
Router(config-if)# cable helper-address 10.10.10.13 host
Router(config-if)# cable helper-address 10.10.10.13 cable-modem
Router(config-if)# exit
Router(config)# exit
Router# show running-config | include helper-address

 cable helper-address 10.10.10.13 cable-modem
```

```
Router#
```

The following example shows that when you specify the **cable-modem** and **host** options with the same IP address on a Cisco uBR10012 router running Cisco IOS Release 12.2(33)SCG and later, it is configured under a bundle interface:

```
Router(config)# interface cable 3/0
Router(config-if)# cable helper-address 10.10.10.13 host
Router(config-if)# cable helper-address 10.10.10.13 cable-modem
Router(config-if)# end
Router# show running-config | include helper-address
cable helper-address 10.10.10.13 cable-modem
cable helper-address 10.10.10.13 host

Router#
```

Related Commands

Command	Description
cable dhcp-giaddr	Modifies the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address before they are forwarded to the DHCP server.
cable relay-agent-option	Enables the system to insert the CM MAC address into a DHCP packet received from a CM or host and forward the packet to a DHCP server.
cable source-verify	Turns on CM upstream verification.
cable telco-return spd dhcp-authenticate	Enforces the telco-return CM to use a specific Dynamic Host Configuration Protocol (DHCP) server.
cable telco-return spd dhcp-server	Identifies the IP address of the Dynamic Host Configuration Protocol (DHCP) server that the telco-return CM must access.
ip dhcp relay information option	Enables the system to insert the CM MAC address into a DHCP packet received from a CM or host and forward the packet to a DHCP server.
ip dhcp smart-relay	Monitors client retransmissions when address pool depletion occurs.

cable host access-group

To configure the access list for a customer premises equipment (CPE) device or host on the Cisco CMTS router, use the **cable host** command in privileged EXEC mode. To remove an access list, use this command with the **no access-group** option.

cable host {*ip-address* | *mac-address*} **access-group** {*access-list* | *access-name*}

cable host {*ip-address* | *mac-address*} **no access-group**

Syntax Description

ip-address	IP address of the CPE device or host.
mac-address	MAC address of the CPE device or host.
access-group	Enables **access-group** options. The **no** form removes access-group specifications.
{*access-list* | *access-name*}	Specifies the IP access list (standard or extended), either by access-list number (1 to 199) or by access-list name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 NA	This command was introduced.
12.2(4)BC1	The functionality of this command was made identical to that of the **cable modem access-group** command, but both commands were retained for backwards compatibility.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

For the **vrf** keyword of this command, only the *ip-address* option is supported.

An access list can be configured to deny access to any IP address other than the ones previously configured, using the **access-list** *access-list* **deny any any** command. Starting with Cisco IOS Release 12.2(33)SCD, when a CM is added to such an access list on the Cisco uBR10012 and Cisco uBR7200 series universal broadband routers, the ping fails. If the CM is reset, removed, or powered off, the ping succeeds after the CM comes online. However, the **show cable modem access-group** command displays that the CM does not belong to the access-group.

Note The **cable host** command, and its SNMP equivalent, cdxCmCpeAccessGroup, are not supported on the Cisco uBR10012 universal broadband router. On this router, use the standard DOCSIS MIB, DOCS-SUBMGT-MIB, instead.

Tip This command is equivalent to configuring cdxCmCpeAccessGroup in CISCO-DOCS-EXT-MIB.

Examples

The following example shows how to assign access list number 2 to the cable host with an IP address of 10.1.1.1:

```
Router# cable host 10.1.1.1 access-group 2
```

Related Commands

Command	Description
clear cable host	Clears the host from the internal address tables of the Cisco CMTS router.
cable device	Configures an access list for a CM device or host on the Cisco CMTS router.
cable modem access-group	Configures the access-group for a CM on the Cisco CMTS router.
show cable device access-group	Display the CMs and the hosts behind the CMs on the network on the Cisco CMTS router.
show cable host access-group	Displays the hosts behind the CMs on the network on the Cisco CMTS router.

cable high-priority-call-window

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:

cable high-priority-call-window *minutes*

no cable high-priority-call-window

Syntax Description

window	This value defines the length of time, in minutes, for which E911 Call History is to be maintained.

Command Default

This command and the PacketCable Emergency 911 Services Listing and History feature is disabled by default on the Cisco CMTS.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(13a)BC	This command was introduced supporting PacketCable Emergency 911 Services Listing and History on the Cisco CMTS: • Cisco uBR7246VXR router • Cisco uBR10012 router
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

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
```

To observe Emergency 911 calls made within the configured window, use the **show cable calls** command in privileged EXEC mode:

The following command example illustrates that one Emergency 911 call was made on the Cable8/1/1 interface on the Cisco uBR10012 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
```

Related Commands

Command	Description
show cable calls	Displays voice call history information and status for the PacketCable Emergency 911 Services Listing and History feature.
show cable modem calls	Displays voice call information for a particular cable modem.

cable igmp static-group

To configure cable per-physical-downstream static multicast support on the Cisco CMTS router, use the **cable igmp static-group** command in global configuration mode.

cable igmp static-group *multicast-group-ip* [**source** *source-ip*] [*subinterface*]

Syntax Description

multicast-group-ip	IP address of the multicast group.
source *source-ip*	(Optional) Source IP address for SSM.
subinterface	(Optional) Subinterface number: • default: 0 for the main interface **Note** If the subinterface is configured at the virtual bundle interface, the subinterface number option for this CLI must be configured to match up with the desired subinterface devices.

Command Default

Cable per-physical-downstream static multicast support is not defined by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

The Cable per-physical-downstream Static Multicast Support feature introduces the concept of a physical IGMP static group, which is an extension of the existing logical IGMP static group. The differences between the two IGMP static groups are:

- A cable bundle logical IGMP static group creates the IGMP static group for the logical IP domain and forwards multicast traffics for the configured multicast group to every slave interface in the same bundle.
- A cable bundle physical IGMP static group creates the IGMP static group on per-physical slave interface basis and will only forwards multicast traffics to only configured slave interfaces.

When an IGMP static group is configured on a master interface, the IGMP static group will perform a check for each slave interface in the multicast group. If the multicast group is configured as a physical static group, then only the corresponding slave interfaces will be added to the cable bundle forwarding table. If the multicast group is configured as a logical static group, then all slave interfaces will be added to the cable bundle forwarding table.

Note When all remaining physical static groups are un-configured from the slave interface for a particular multicast group on a particular bundle, the Cisco CMTS router will revert back to the logical static group for that multicast group on that bundle.

DSG Usage

The **cable igmp static-group** command will only appear in the output of the **show running-configuration** command if it is configured via the CLI. If it is configured by DSG, the **cable igmp static-group** command CLI will remain hidden for a particular multicast group. This is done in order to eliminate any confusion with the current DSG configurations.

Note Any multicast group being used by DSG (or CLI) within the same CMTS, should not be used for CLI (or DSG) configuration.

Examples

The following example shows the **cable igmp static-group** command on the Cisco CMTS router:

```
Router(config-if)# cable igmp static-group 230.1.1.1
```

The following example shows the **cable igmp static-group** command with the **source** option on the Cisco CMTS router:

```
Router(config-if)# cable igmp static-group 232.1.1.1 source 10.1.1.1
```

Related Commands

Command	Description
ip igmp static-group	Configure static group membership entries on an interface.

cable init-channel-timeout

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 Multipart Registration Response (REG-RSP-MP) messages, use the **cable init-channel-timeout** command in cable interface configuration mode. To disable this configuration, use the **no** form of this command.

cable init-channel-timeout *value*

no cable init-channel-timeout *value*

Syntax Description

value	Channel timeout value in seconds. Valid range is from 10 to 180 seconds. The default value is 60.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCC	This command was introduced in Cisco IOS Release 12.2(33)SCC.

Examples

The following example shows how to specify the channel timeout value on a cable interface at slot/subslot/port 5/1/0 on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 5/1/0
Router(config-if)# cable init-channel-timeout 90
```

cable insertion-interval

To configure the interval between consecutive initial ranging slots on an upstream, use the **cable insertion-interval** interface configuration command. To configure the automatic setting and ignore any minimum or maximum time settings, use the **no** form of this command.

cable insertion-interval {**fixed-intrvl** | **automatic** [*min-intrvl*] [*max-intrvl*]}

no cable insertion-interval

Syntax Description

fixed-intrvl	Fixed interval between initial ranging slots in milliseconds. The valid range is 100 to 2000 milliseconds.
automatic	Causes the Cisco CMTS MAC scheduler for each upstream CM to vary the initial ranging times available to new CMs joining the network.
min-intrvl	(Optional) Minimum value in milliseconds between the initial ranging slots on the upstream. The valid range is 20 to 120, with a default of 60 milliseconds.
max-intrvl	(Optional) Maximum value in milliseconds between the initial ranging slots on the upstream. The valid range is 240 to 1800, with a default of 480 milliseconds.

Command Default

Automatic (dynamically varying the frequency of initial ranging upstream slots between 60 milliseconds and 480 milliseconds)

Command Modes

Interface configuration—cable interface only (config-if)

Command History

Release	Modification
11.NA	This command was introduced.
12.1 T	This command was modified.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA)	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

Use this command to specify the minimum and maximum duration between initial ranging opportunities that appear in MAP messages sent by the Cisco CMTS router. MAP messages define the precise time intervals during which CMs can send.

The default insertion interval setting (**automatic**) configures the Cisco CMTS router to optimize the initial ranging times available to new CMs that attempt to join the network. The optimization algorithm automatically varies the initial ranging times between 60 and 480 milliseconds, depending on the number of CMs attempting to come online.

Use the **cable insertion-interval automatic** command to bring a large number of CMs online quickly (for example, after a major power failure). After the CMs have come online, you can override the **automatic** keyword by giving this command again and specifying a specific insertion interval.

Examples

The following example shows the default configuration, which is to specify automatic insertion intervals, using the default initial ranging intervals:

```
Router# configure terminal
Router(config)# interface cable 3/0
Router(config-if)# cable insertion-interval automatic
```

The following example shows how to set the minimum insertion interval to 100 ms:

```
Router# configure terminal
Router(config)# interface cable 5/1/0
Router(config-if)# cable insertion-interval 100
```

Related Commands

Command	Description
cable upstream data-backoff	Specifies automatic or fixed start and stop values for data backoff.
cable upstream range-backoff	Specifies automatic or configured initial ranging backoff calculation.

cable intercept

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

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

no cable intercept *mac-address*

Syntax Description

mac-address	Specifies the MAC address to be intercepted. For Cisco uBR10012 router, a maximum of 4095 MAC addresses can be configured. For Cisco uBR7200 series router, a maximum of 10 MAC addresses per interface can be configured.
ip-address	Specifies the IP address for the destination data collector.
udp-port	Specifies the destination UDP port number for the intercept stream at the data collector. Valid range is 0 to 65535.

Command Default

Disabled

Command Modes

Interface configuration—cable interface only (config-if)

Command History

Release	Modification
12.0(5)T1	This command was introduced.
12.0(6)SC	This command was introduced on the 12.0 SC train.
12.1(2)EC	This command was introduced on 12.1 EC train.
12.1(11b)EC	Support was added to allow the data collector to be more than two hops from the Cisco CMTS router.
12.2(4)BC1	This command was integrated into Cisco IOS Release 12.2(4)BC1.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SCC	This command was modified. The command is now configured under bundle interface.

Usage Guidelines

When this command is activated, the Cisco CMTS router examines each packet for the desired MAC address; when a matching MAC address is found (for either the origination or destination endpoint), a copy of the packet is encapsulated into a UDP packet, which is then sent to the specified server at the given IP address and port.

Note The data collecting system at the *ip-address* on the *udp-port* must be configured to listen for and capture the necessary data stream. An IP route to the specified IP address must exist, and IP connectivity to that device must be present for the traffic to be captured. Before Cisco IOS Release 12.1(11b)EC, the data collecting system must be within two routing hops of the Cisco CMTS.

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 Service Independent Intercept [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.

This command is originally designed to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other law enforcement wiretap requirements for voice communications. For additional information, see the *PacketCable Electronic Surveillance Specification*, which is available at the following URL at the PacketCable web site: http://www.packetcable.com.

Note For lawful intercept, it is recommended to use SII (through SNMPv3) instead of the **cable intercept** command.

Note Starting from Cisco IOS Release 12.2(33)SCC, the **cable intercept** command is configured under bundle interface.

Examples

The following commands specify that a copy of all traffic for the CPE with the MAC address of 0080.fcaa.aabb should be forwarded to the data collector that is listening at UDP port 512 at the IP address of 10.12.13.8. The **show interface cable intercept** command displays which intercepts are currently active.

```
Router# configure terminal
Router#(config) interface cable 6/0
Router(config-if)# cable intercept 0080.fcaa.aabb 10.12.13.8 512
Router(config-if)# exit
Router(config)# exit
Router# show interface cable 6/0 intercept
                Destination   Destination
MAC Address     IP Address    UDP Port
0080.fcaa.aabb  3.12.13.8      512
```

The following example shows the behavior of the **cable intercept** command that is configured under bundle interface. The **show running interface** command displays which intercepts are currently active.

```
Router# configure terminal
Router#(config) interface bundle 10
Router(config-if)# cable intercept 0080.fcaa.aabb 10.12.13.8 512
Router(config-if)# exit
Router(config)# exit
Router# show running interface bundle 10 | i intercept
cable intercept 0080.fcaa.aabb 10.12.13.8 512
```

Related Commands

Command	Description
cable monitor	Enables the forwarding of selected packets on the cable interface to an external LAN analyzer.
show interface cable intercept	Displays the CMs for which cable intercept is currently active.

cable ip-init

To configure the IP provisioning mode supported by the cable interface on a Cisco CMTS router, use the **cable ip-init** command in interface or subinterface configuration mode. To remove the IP provisioning configuration, use the **no** form of this command.

cable ip-init {**apm** | **dual-stack** | **ipv4** | **ipv6**}

no cable ip-init {**apm** | **dual-stack** | **ipv4** | **ipv6**}

Syntax Description

apm	Configures the interface to support Alternative Provisioning Mode (APM).
dual-stack	Configures the interface to support both IPv4 and IPv6 addressing.
ipv4	Configures the interface to support IPv4 address only.
ipv6	Configures the inerface to support IPv6 address only.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCA	This command was introduced.
12.2(33)SCC	This command was modified. The **apm** keyword was added.

Usage Guidelines

The **cable ip-init** command configures the cable interface for the IP addressing mode that it supports. This information is included in the IP initialization parameters of the MAC Domain Descriptor (MDD) message.

Examples

The following example shows how to configure a cable interface on a Cisco CMTS router to support both IPv4 and IPv6 addressing:

```
interface cable 5/0/1
 cable ip-init dual-stack
```

cable ip-broadcast-echo

To activate upstream IP broadcast echo so that the Cisco CMTS router can echo broadcast packets, use the **cable ip-broadcast-echo** command in cable interface or subinterface configuration mode. To disable the upstream IP broadcast echo, use the **no** form of this command.

cable ip-broadcast-echo

no cable ip-broadcast-echo

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Cable interface and subinterface configuration (config-if)

Command History

Release	Modification
11.3 XA	This command was introduced.
12.1(3a) EC	The subinterface support was added.
12.1(5)EC	Support was added for the Cisco uBR7100 series routers.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

By default, broadcast IP packets that arrive on the upstream at the Cisco CMTS router are not forwarded on the downstream ports so that they would be delivered to the other CMs and CPE devices. This behavior prevents broadcast storms in which such packets are repeatedly looped through the network.

The **cable ip-broadcast-echo command** changes this behavior by forwarding such packets on the appropriate downstream ports, so that the packet is received by all CMs and CPE devices on that segment of the network. This allows the cable network to behave more like a standard Ethernet network, and support direct peer-to-peer communications using IP broadcasts.

Note This command should not be used in a typical service provider network.

Examples

The following example shows how to activate IP broadcast echo in the cable interface configuration mode:

```
Router(config-if)# cable ip-broadcast-echo
```

The following example shows how to activate IP broadcast echo in the cable subinterface configuration mode:

```
Router(config)# interface cable 6/0.1
Router(config-subif)# cable ip-broadcast-echo
```

Related Commands

Command	Description
cable ip-multicast-echo	Enables IP multicast echo so that the Cisco CMTS can echo multicast packets.

cable ip-multicast-echo

To enable IP multicast echo so that the Cisco CMTS can echo multicast packets, use the **cable ip-multicast-echo** command in cable interface configuration mode. To disable IP multicast echo, use the **no** form of this command.

cable ip-multicast-echo

no cable ip-multicast-echo

Syntax Description

This command has no arguments or keywords.

Command Default

IP multicast echo is disabled by default.

Command Modes

Cable interface configuration (config-if)

Command History

Release	Modification
11.3 XA	This command was introduced for Cisco uBR7200 series routers.
12.1(3a) EC	The subinterface support was added.
12.1(5)EC	Support was added for Cisco uBR7100 series routers.
12.2(4)BC1	Support was added for the Cisco uBR10012 router.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SCB	The command default is changed to disabled in Cisco IOS Release 12.2(33)SCB and later.

Usage Guidelines

By default, 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.

This behavior might not be appropriate for certain applications or networks, so the **no cable ip-multicast-echo command** changes this behavior by preventing the forwarding of multicast packets. Disabling multicast traffic can prevent some types of broadcast storms in which such packets are repeatedly looped through the network.

To verify if IP multicast echo has been activated or deactivated, enter the **show running-config** command and look for the cable interface configuration information.

If IP multicast echo is enabled, it appears in this output of the **show running-config** command.

If IP multicast echo is disabled, it is not displayed in the output **show running-config** command.

If you are having trouble, make sure that you have entered the correct slot and port numbers when you entered cable bundle interface configuration mode.

Note 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.

Examples

The following example shows how to disable IP multicast echo in the bundle interface configuration mode:

```
Router(config-if)# no cable ip-multicast-echo
```

Related Commands

Command	Description
cable ip-broadcast-echo	Enables upstream IP broadcast echo so that the Cisco CMTS can echo broadcast packets.

cable ipc-stats

To enable the Cable IPC Statistics Collection tool on a Cisco CMTS router, use the **cable ipc-stats** command in global configuration mode. To disable this configuration, use the **no** form of this command.

cable ipc-stats

no cable ipc-stats

Syntax Description

This command has no arguments or keywords.

Command Default

The Cable IPC Statistics Collection tool is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCC	This command was introduced in Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

The Cable IPC Statistics Collection tool provides debugging information about all IPC messages. 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 **cable ipc-stats** command is synchronized on all cable interface line cards from the active RP. You do not have to use this command on cable interface line cards separately.

Examples

The following example shows how to enable the Cable IPC Statistics Collection tool on a Cisco CMTS router:

```
Router# configure terminal
Router(config)# cable ipc-stats
```

Related Commands

Command	Description
clear cable ipc-stats	Clears the active database and resets IPC statistics in the active database to zero.
show cable ipc-stats	Displays statistics of all the IPC messages on a Cisco CMTS router.

cable ipv6 source-verify

To enable source verification of IPv6 packets received by a cable interface upstream on a Cisco CMTS router, use the **cable ipv6 source-verify** command in bundle interface or subinterface configuration mode. To disable IPv6 source verification, use the **no** form of this command.

cable ipv6 source-verify [**dhcp** [**server** *ip-address*] | **leasequery-filter upstream** *threshold interval* | **leasetimer** *value*]

no cable ipv6 source-verify

Syntax Description

dhcp	(Optional) Verifies IP address with the DHCPv6 server. • **server**—Enables the Leasequery server to send the DHCPv6 Leasequeries. • *ip-address*—IPv6 address of the Leasequery server.
leasequery-filter	(Optional) Filters the IPv6 Leasequery requests. • **upstream**—Indicates that the Leasequery requests are sent on cable upstream interfaces. • *threshold*—Maximum number of DHCP Leasequeries allowed per SID for each interval period. The valid range is from 0 to 55. • *interval*—Time period, in seconds, when Leasequeries should be monitored. The valid range is from 1 to 5 seconds.
leasetimer	(Optional) Specifies the time, in minutes, when the router should check its internal CPE database for IP addresses whose lease times has expired. • *value*—Lease time value. The valid range is from 1 to 240 minutes, with a default of 60 minutes.

Command Default

IPv6 source verification is disabled.

Command Modes

Bundle interface configuration (config-if),

Bundle subinterface configuration (config-subif)

Command History

Release	Modification
12.2(33)SCA	This command was introduced.
12.2(33)SCF1	This command was modified. The **dhcp** keyword was added to verify IPv6 address with the DHCPv6 server. The **leasequery-filter** and **leasetimer** keywords were added to further filter the IPv6 Leasequery requests.

Usage Guidelines

The IPv6 source verification feature is enabled on a cable bundle interface or subinterface.

When you enable IPv6 source verification on the Cisco CMTS bundle interface, the source verification routine is run to verify the MAC-SID-IP binding of the packet. If the source verification succeeds, the packet is forwarded. If the verification fails, then the packet is dropped.

When a cable modem (CM) is operating as a bridged modem device, then the Cisco CMTS router verifies the entire IPv6 address for that CM and the CPEs behind that CM.

When a CM is operating as a router modem device, then the Cisco CMTS router only verifies the network prefix for that CM and the CPEs behind that CM. To be successful, this means that all cable modem routers must have different prefixes assigned to them.

The **cable ipv6 source-verify** command only controls the source verification of IPv6 packets. For IPv4-based source verification, you must use the **cable source-verify** command, which also supports

Note On the Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCA, source verification of IPv6 packets occurs only on packets in the process-switched path of the route processor (RP).

Using the dhcp Option

If the **dhcp** option is used, the Cisco CMTS sends a DHCPv6 Leasequery message to the DHCP server to verify the IP address. If a valid response is received from the DHCP server, the Cisco CMTS updates its database with the new CPE device and allows future traffic through. If the DHCP server does not return a successful response, all traffic from the CPE is dropped.

If you are using the **dhcp** option, you have the option to specify an alternate DHCP server using its IP address. The **dhcp** option supports source verification from multiple dhcp servers.

For single dhcp server, use the command **cable ipv6 source-verify dhcp** [**server** *ipv6-address*] command. For multipledhcp servers use the command **cable ipv6 source-verify dhcp** command.

Using the leasetimer Option

The **leasetimer** option adds another level of verification by activating a timer that periodically examines the lease times for the IP addresses for known CPE devices. If the Cisco CMTS discovers that the DHCP lease for a CPE device has expired, it removes that IP address from its database, preventing the CPE device from communicating until it makes another DHCP request. This prevents users from treating DHCP-assigned addresses as static addresses, as well as from using IP addresses that were previously assigned to other devices.

The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface. Also, this option is supported only on the primary bundle interface and cannot be configured on subinterfaces. Configuring it for a primary bundle interface automatically applies it to all subinterfaces.

Using the leasequery-filter Option

To prevent a large volume of Leasequery requests on a cable interface, use the **cable ipv6 source-verify leasequery-filter** command. After configuring this command, the Cisco CMTS allows only the configured number of DHCPv6 Leasequery requests within the specified interval time period.

For example, the **cable ipv6 source-verify leasequery-filter 5 10** command configures the Cisco CMTS so that the Cisco CMTS allows a maximum of five DHCPv6 Leasequery requests every 10 seconds for each SID.

Examples

The following example shows how to enable IPv6 source verification on a Cisco CMTS router bundle interface by first configuring cable ipv6 source-verify at the bundle interface:

```
interface bundle 1
 cable ipv6 source-verify
```

After you configure the bundle interface, associate the bundle at the cable interface:

```
interface cable 6/0/2
 cable bundle 1
```

The following example shows how to configure the Cisco CMTS router to send DHCPv6 Leasequeries to verify unknown source IP addresses in upstream data packets. Both **cable ipv6 source-verify dhcp** and **no cable nd** commands must be configured on the Cisco CMTS bundle before the Cisco CMTS will issue any DHCPv6 Leasequery to recover an unknown IPv6 CPE to the Cisco CMTS.

```
configure terminal
 interface bundle 1
  cable ipv6 source-verify dhcp
  no cable nd
```

The following example shows how to configure the leasetimer option so that the Cisco CMTS checks the IP addresses in the CPE database for that particular interface for expired lease time:

```
configure terminal
 interface bundle 1
  cable ipv6 source-verify dhcp
  cable ipv6 source-verify leasetimer 120
```

The following example shows how to configure the Cisco CMTS router so that it allows a maximum of five DHCP Leasequery requests per SID over each 2-second interval on a particular cable interface.

```
configure terminal
 interface bundle 1
  cable ipv6 source-verify dhcp
  cable ipv6 source-verify leasequery-filter 5 2
```

Associated Features

The **cable ipv6 source-verify** command is used to configure the following feature:

- Cable DHCP Leasequery

Related Commands

Command	Description
cable source-verify	Enables verification of IPv4 addresses for CMs and CPE devices on an upstream.
cable ipv6 source-verify leasequery-filter downstream	Enables the Leasequery filter in the CMTS downstream for IPv6 packets.

cable ipv6 source-verify leasequery-filter downstream

To enable the Leasequery filter on the Cisco CMTS downstream for IPv6 packets, use the **cable ipv6 source-verify leasequery-filter downstream** command in global configuration mode. To disable the Leasequery filter on the Cisco CMTS downstream, use the **no** form of this command.

cable ipv6 source-verify leasequery-filter downstream *threshold interval*

no cable ipv6 source-verify leasequery-filter downstream

Syntax Description

downstream	Filters the IPv6 Leasequery requests on the Cisco CMTS downstream. • *threshold*—Maximum number of DHCP Leasequeries allowed for unknown SIDs for each interval period. The valid range is from 0 to 255. • *interval*—Time period, in seconds, when Leasequeries should be monitored. The valid range is from 1 to 10 seconds.

Command Default

IPv6 source verification for downstream is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCF1	This command was introduced.

Usage Guidelines

Use the **cable ipv6 source-verify leasequery-filter downstream** command to enable the Leasequery filter on the Cisco CMTS downstream for IPv6 packets.

Examples

The following example shows how to enable the Leasequery filter on the CMTS downstream for IPv6 packets on all downstream cable interfaces.

```
Router# configure terminal
Router(config)# cable ipv6 source-verify leasequery-filter downstream 10 5
```

Associated Features

The **cable ipv6 source-verify leasequery-filter downstream** command is used to configure the following feature:

- Cable DHCP Leasequery

Related Commands

Command	Description
cable ipv6 source-verify	Enables source verification of IPv6 packets received by a cable interface upstream on a Cisco CMTS router.