



Cable Commands: cable s

Revised: March 30, 2009, OL-15510-09

New Commands

Command	Cisco IOS Software Release
cable service attribute ds-bonded downstream-type bonding-enabled	12.3(23)BC
cable service attribute non-ds-bonded downstream-type bonding-disabled	12.3(23)BC
cable service attribute non-ds-bonded legacy-ranging downstream-type	12.3(23)BC
cable service attribute voice-enabled	12.3(23)BC
cable service type	12.2(33)SCB
cable submgmt default	12.2(33)SCB

Modified Commands

Command	Cisco IOS Software Release
cable service class	12.2(33)SCB
cable service class	12.2(33)SCB1

cable service attribute ds-bonded downstream-type bonding-enabled

To force a downstream bonding-capable modem to initialize on a bonded primary-capable downstream channel, use the **cable service attribute ds-bonded downstream type bonding-enabled** command in global configuration mode. To restore default configuration, use the **no** form of the command.

cable service attribute ds-bonded downstream-type bonding-enabled [enforce]

no cable service attribute ds-bonded downstream-type bonding-enabled

Syntax Description	enforce	Enforces bonding-capable modems to register only on bonded RF channels.
---------------------------	---------	---

Command Default	A bonding-capable modem is allowed to register on the primary channel selected by the modem for initiation even if the channel is not part of a bonding group.	
------------------------	--	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.3(23)BC	This command was introduced for the uBR10012 router.

Usage Guidelines	<p>For bonding capable cable modems, the primary channel selection that is done by the CMTS depends on whether the modems can resolve its MAC Domain Downstream Service Group ID (MD-DS-SG). The CM must attempt to determine its MAC Domain Downstream Service Group ID (MD-DS-SG-ID) if an MDD is present on the downstream. If a modem has resolved its MD-DS-SG, the CMTS selects a bonded primary channel, the primary channel that is part of an operational wideband channel, from the RF channel set corresponding to the MD-DS-SG determined by the modem. The bonded primary channel selected by the CMTS needs to be hosted by an interface on the same uBR10-MC5X20 cable interface line card as the modem's initial primary channel. If there are multiple primary capable channels that meet the above criteria, the final primary channel will be randomly selected among the eligible channel set.</p>
-------------------------	--

If a modem has not resolved its MD-DS-SG and the enforce option is configured, the CMTS selects a bonded primary channel based on MAP group associated with the modem's upstream channel. Typically, an upstream channel is configured into a single fiber node and the CMTS infers the topology information based on the downstream channels associated with the upstream. If the enforce option is not configured or the CMTS cannot find a target primary channel, the modem will be allowed to register on the primary channel currently selected by the modem for initialization.



Note	The CMTS will only try to move the modem with MD-DS-SG unresolved if the enforce option is configured.
-------------	---

By default, changing the primary channel to select a wideband channel is not enforced and modems are allowed to operate on a primary channel even if they are not included in any load balancing groups. At any time after the system is up, enabling the primary channel selection for bonding capable modems will not affect existing modems in the system. The operator has to manually reset the bonding capable modems using the **clear cable modem** command either globally or at per-MAC Domain level.

**Note**

Enabling primary channel selection for wideband modems will not affect existing modems in the system.

Examples

```
Router# configure terminal
Router(config)# cable service attribute ds-bonded downstream-type bonding-enabled [enforce]
```

Related Commands

cable service attribute voice-enabled	Restricts voice services to only to the uBR10-MC5x20 line cards for high availability.
cable service attribute non-ds-bonded downstream-type bonding-disabled	Forces the non-bonding-capable modems to register only on non-bonded RF channels on the CMTS.

cable service attribute non-ds-bonded downstream-type bonding-disabled

To force the non-bonding-capable modems to register only on non-bonded RF channels on the CMTS, use the **cable service attribute non-ds-bonded downstream-type bonding-disabled** command in global configuration mode. To restore default behavior, use the **no** form of the command.

cable service attribute non-ds-bonded downstream-type bonding-disabled

Syntax Description This command has no keywords or arguments.

Command Default The non-bonding-capable modem registers on its current primary channel.

Command Modes Global configuration

Command History

Release	Modification
12.3(23)BC	This command was introduced for the Cisco uBR10012 router.

Usage Guidelines

A modem is identified as a non-bonding-capable modem if the modem reports a Multiple Receive Channel Support value of 1 for TLV 5.29 or an RCP ID unknown to the CMTS during the modem's registration request.

The non-bonding capable modem, identified at registration, will be moved to a non-bonded primary channel through downstream frequency override, if its current primary channel is part of a bonding group. The target non-bonded primary channel will be selected among primary capable channels that are associated to the modem's current upstream channel, however not included in any wideband channels associated to any host interfaces on the local line card. Once this option is enabled, the bonded primary channels will be taken out of load balancing group, to prevent non-bonding capable modems to be moved back to bonded primary channels for load balancing purpose.



Note

Enabling primary channel selection for wideband modems will not affect existing modems in the system. The operator has to reset the existing non-bonding capable modems using the **clear cable modem** command.

Examples

```
Router# configure terminal
Router(config)# cable service attribute non-ds-bonded downstream-type bonding disabled
```

Related Commands		
	cable service attribute voice-enabled	Restricts voice services to only to the uBR10-MC5x20 line cards for high availability.
	cable service attribute ds-bonded downstream-type bonding-disabled	Forces a downstream bonding-capable modem to initialize on a bonded primary-capable downstream channel.
	clear cable modem	Removes all modems or modems hosted by a uBR10-MC5x20 downstream interface under a specific category.

cable service attribute non-ds-bonded legacy-ranging downstream-type

To redirect potential non-bonding-capable modems that access the CMTS with INIT-RNG_REQ at initialization to a specified downstream channel frequency, use the **cable service attribute non-ds-bonded legacy-ranging downstream-type command** in global configuration mode. To restore default behavior, use the **no** form of the command.

cable service attribute non-ds-bonded legacy-ranging downstream-type frequency *freq*

no cable service attribute legacy-ranging downstream-type

Syntax Description

frequency *freq* Specifies the downstream channel frequency to which modems that access the CMTS with legacy INIT-RNG-REQ are moved.

Command Default

The non-bonding-capable modem continues the ranging process on the primary channel currently selected by the modem for initialization.

Command Modes

Global configuration

Command History

Release	Modification
12.3(23)BC	This command was introduced for the uBR10012 router.

Usage Guidelines

The **cable service attribute non-ds-bonded** command provides the ability to prevent potential non-bonding-capable modems that access CMTS with legacy INIT-RNG-REQ at initialization to register on a CMTS that supports bonding-capable modem. These modems that use legacy initial ranging will be redirected to a specified downstream channel frequency.



Note

If the frequency option is used and if the frequency is modified, then the new frequency setting will only impact new modems trying to initialize after the frequency is modified. To enforce the downstream channel selection policy on existing modems, each modem has to be manually reset either globally or at the individual primary channel level using the **clear cable modem** command.

Examples

```
Router# configure terminal
Router(config)# cable service attribute non-ds-bonded legacy-ranging downstream-type frequency
55000000
```

Related Commands	
cable service attribute voice-enabled	Restricts voice services only to the uBR10-MC5x20 line cards for high availability.
cable service attribute ds-bonded downstream-type bonding-enabled	Forces a downstream-bonding capable modem to initialize on a bonded primary-capable downstream channel.
cable service attribute non-ds-bonded downstream-type bonding-disabled	Forces the non-bonding-capable modems to register only on non-bonded RF channels on the CMTS.
clear cable modem	Removes all modems or modems hosted by a uBR10-MC5x20 line card downstream interface under a specific category.

cable service attribute voice-enabled

To restrict voice services only to the uBR10-MC5X20 downstream interfaces for high availability, use the **cable service attribute voice-enabled** command in global configuration mode. To remove the restriction of voice services to the uBR10-MC5X20 downstream interfaces, use the **no** form of the command.

cable service attribute voice-enabled downstream-type HA-capable

no cable service attribute voice-enabled downstream-type HA-capable

Syntax Description

downstream-type	Restricts voice services to a specific downstream type.
HA-capable	Restricts voice services to the uBR10-MC 5x20 line card.

Command Default

All primary-capable downstream channels on the uBR10-MC 5x20 line card and the SPA can support downstream voice service flows.

Command Modes

Global configuration

Command History

Release	Modification
12.3(23)BC	This command was introduced for the Cisco uBR10012 router.

Usage Guidelines

A voice-enabled cable modem is identified either at registration by decoding DHCP TLV 122 in the modem's DHCP-ACK, or at its first voice call if DHCP TLV 122 is not exchanged. If a voice-enabled modem is detected at registration on a SPA downstream channel, it will be moved to the uBR10-MC5x20 downstream channel in the CGD *via* downstream frequency override. If the voice-enabled modem is detected at its first voice call after registration, it will be moved after the call is over to the uBR10-MC5x20 channel in the CGD *via* DCC. If the voice enabled modem fails to come up on the target uBR10-MC5x20 channel, the CMTS will continue to move the modem until three retries (the maximum number of allowed retries) has been reached, when the modem will be allowed to stay on the SPA downstream channel until another set of retries is attempted by the CMTS every 24 hours. A voice enabled modem on the uBR10-MC5x20 channel will be excluded from being load balanced to a SPA downstream channel. If this option is configured at any time after the system is up, voice enabled modems that have been identified on the SPA downstream channel without active voice calls will be gradually moved to the uBR10-MC5x20 downstream channel in the CGD at the rate of one modem per five seconds.

Examples

```
Router# configure terminal
Router(config)# cable service attribute voice-enabled downstream-type HA-capable
```

Related Commands

cable service attribute non-ds-bonded	Forces a non-bonding-capable modem to register only on non-bonded RF channels.
cable service attribute ds-bonded	Forces a downstream-bonding capable modem to initialize on a bonded primary-capable DS channel.

cable service class

To set parameters for DOCSIS 1.1 cable service class, use the **cable service class** command in global configuration mode. To delete a service class or to remove a configuration, use the **no** form of the command.

cable service class *class-index* [*keyword-options*]

no cable service class *class-index* [*keyword-options*]

Syntax Description

<i>class-index</i>	Specifies the class ID for the class to be modified. Valid range is 1 to 255.
activity-timeout	Specifies the activity timeout (0 to 65,535).
admission-timeout	Specifies the admitted timeout (0 to 65,535).
downstream	Specifies that the service class is for the downstream direction (from the CMTS to the CM). (The default direction is upstream .)
grant-interval	Specifies the grant interval (0 to 4,294,967,295 microseconds).
grant-jitter	Specifies the grant jitter (0 to 4,294,967,295 microseconds).
grant-size	Specifies the grant size (0 to 65,535 bytes).
grants-per-interval	Specifies the grants per interval (0 to 127 grants).
max-burst	Specifies the maximum transmission burst (1522 to 4,294,967,295 bytes). Note The recommended value range is 1600 to 1800 bytes. Using a value of 0 or greater than 1800 bytes can cause latency issues for Voice-over-IP. A value of less than 1522 bytes can prevent the upstream transmission of large ethernet frames for any CM or CMTS not implementing fragmentation.
max-concat-burst	Specifies the maximum concatenation burst (0 to 65,535 bytes).
max-latency	Specifies the maximum latency allowed (0 to 4,294,967,295 microseconds).
max-rate	Specifies the maximum rate (0 to 4,294,967,295 bps).
min-packet-size	Specifies the minimum packet size for reserved rate (0 to 65,535 bytes).
min-rate	Specifies the minimum rate (0 to 4,294,967,295 bps).
name	Specifies the service class name string.
peak-rate	Specifies the peak rate (0 to 4,294,967,295 bps). Default value is zero, which represents the line rate. Note The <i>peak-rate</i> option is not supported on the DOCSIS 1.0 modems.
poll-interval	Specifies the poll interval (0 to 4,294,967,295 microseconds).
poll-jitter	Specifies the poll jitter (0 to 4,294,967,295 microseconds).
priority	Specifies the priority (0 to 7, where 7 is the highest priority).
req-trans-policy	Specifies the request transmission policy bit field (0 to FFFFFFFF in hexadecimal).

sched-type	Specifies the service class schedule type: 2–Best-Effort Schedule Type 3–Non-Real-Time Polling Service Schedule Type (supported only in Cisco 12.2(4)BC and later releases) 4–Real-Time Polling Service Schedule Type 5–Unsolicited Grant Service with Activity Detection Schedule Type 6–Unsolicited Grant Service Schedule Type
tos-overwrite <i>and-mask or-mask</i>	Overwrites the ToS byte by first ANDing the TOS value with the <i>and-mask</i> value and then ORing the result of that operation with the <i>or-mask</i> value. Both parameters must be specified in hexadecimal. The <i>and-mask</i> value can range from 0x0 to 0xFF and the <i>or-mask</i> value can range from 0x0 to 0xFF.
upstream	Specifies that the service class is for the upstream direction (from the CM to the CMTS). This is the default direction.
<i>n</i>	Specifies the bundle identifier.
req-attr-mask	Specifies the required attribute mask bit field (0 to FFFFFFFF in hexadecimal).
forb-attr-mask	Specifies the forbidden attribute mask bit field (0 to FFFFFFFF in hexadecimal).

Command Default

Values that are not specified are set to their DOCSIS 1.1 defaults, if applicable to the service-class schedule type. See Section C.2.2, *Service Flow Encodings*, in the DOCSIS 1.1 specification.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(4)CX	This command was introduced for DOCSIS 1.1 operation. This command replaced the cable qos profile command that was used in previous versions for DOCSIS 1.0 operation.
12.2(4)BC1	This command was integrated into Cisco IOS release 12.2(4)BC1. This command was also enhanced to support NRTPS scheduling.
12.2(11)BC2	The default value for the maximum transmission burst parameter (max-burst) was changed from 1522 bytes to 3044 bytes. The default value for the maximum concatenation burst parameter was also changed from 0 bytes (unlimited) to 1522 bytes. These changes are to accommodate the latest revision of the DOCSIS 1.1 specification (SP-RFI-v1.1-I09-020830).
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.
12.2(33)SCB	This command was modified with the addition of req-attr-mask and forb-attr-mask keywords.
12.2(33)SCB1	This command was modified with the addition of <i>peak-rate</i> to set value greater than the <i>max-rate</i> .

Usage Guidelines

The **sched-type** option must always be specified for each class. When a certain scheduling type is selected, take care that the mandatory parameters for that scheduling type are explicitly entered, while nonapplicable parameters must be explicitly removed.

The default direction is **upstream**. We recommend that you do not change the direction of a service class after you have created it, because some of the existing service class parameters might not be appropriate for the new direction. Instead, delete the current service class and create a new service class with the correct upstream or downstream direction.

If the service class is newly created, a service-class name must be defined before entering the parameters for the service class.

**Note**

Section C.2.2.6.10, *IP Type of Service Overwrite*, of the DOCSIS 1.1 specification changed the operation of **tos-overwrite** option. In DOCSIS 1.1 networks, the new TOS value is calculated by the following formula: New IP TOS = ((Original TOS value AND *and-mask*) OR *or-mask*). (For a description of the previous method of calculating the TOS value, see the **cable qos profile** command.) The default is to leave the TOS value unchanged (no overwrite).

Examples

The following examples show configurations that use the **cable service class** command to create service classes. Based on the scheduling type specified, some command lines are mandatory, while others are optional.

Each example shown here is a complete configuration set for creating a service class.

Configuring a Service Class for Unsolicited Grant Scheduling Service

```
Router(config)# cable service class 1 name UP_UGS
Router(config)# cable service class 1 sched-type 6
Router(config)# cable service class 1 grant-size 100
Router(config)# cable service class 1 grant-interval 20000
Router(config)# cable service class 1 grant-jitter 4000
Router(config)# cable service class 1 grants-per-interval 1
Router(config)# cable service class 1 min-packet-size 100
Router(config)# cable service class 1 req-trans-policy 0x1FF
Router(config)# cable service class 1 tos-overwrite 0x1F 0xE0
Router(config)# cable service class 1 activity-timeout 30
Router(config)# cable service class 1 admission-timeout 30
```

Configuring a Service Class for Unsolicited Grant Scheduling with Activity Scheduling

```
Router(config)# cable service class 2 name UP_UGSAD
Router(config)# cable service class 2 sched-type 5
Router(config)# cable service class 2 grant-size 100
Router(config)# cable service class 2 grant-interval 20000
Router(config)# cable service class 2 grant-jitter 4000
Router(config)# cable service class 2 grants-per-interval 1
Router(config)# cable service class 2 poll-interval 10000
Router(config)# cable service class 2 poll-jitter 4000
Router(config)# cable service class 2 min-packet-size 100
Router(config)# cable service class 2 req-trans-policy 0x1FF
Router(config)# cable service class 2 tos-overwrite 0x1F 0xE0
Router(config)# cable service class 2 activity-timeout 30
Router(config)# cable service class 2 admission-timeout 30
```

Configuring a Service Class with Real-Time Polling Service

```
Router(config)# cable service class 3 name UP RTPS
Router(config)# cable service class 3 sched-type 4
```

```

Router(config)# cable service class 3 poll-interval 10000
Router(config)# cable service class 3 poll-jitter 4000
Router(config)# cable service class 3 min-rate 64000
Router(config)# cable service class 3 max-rate 128000
Router(config)# cable service class 3 max-burst 2000
Router(config)# cable service class 3 max-concat-burst 1522
Router(config)# cable service class 3 req-trans-policy 0x1FF
Router(config)# cable service class 3 tos-overwrite 0x1F 0xE0
Router(config)# cable service class 3 activity-timeout 30
Router(config)# cable service class 3 admission-timeout 30

```

Configuring a Service Class for Best-Effort Upstream Service

```

Router(config)# cable service class 4 name UP_BE
Router(config)# cable service class 4 sched-type 2
Router(config)# cable service class 4 priority 5
Router(config)# cable service class 4 min-rate 0
Router(config)# cable service class 4 max-rate 128000
Router(config)# cable service class 4 max-burst 2000
Router(config)# cable service class 4 max-concat-burst 1522
Router(config)# cable service class 4 req-trans-policy 0x0
Router(config)# cable service class 4 tos-overwrite 0x1F 0xE0
Router(config)# cable service class 4 activity-timeout 30
Router(config)# cable service class 4 admission-timeout 30

```

Configuring a Service Class for Best-Effort Downstream Service

```

Router(config)# cable service class 5 name DOWN_BE
Router(config)# cable service class 5 priority 5
Router(config)# cable service class 5 min-rate 0
Router(config)# cable service class 5 max-rate 1000000
Router(config)# cable service class 5 max-burst 3000
Router(config)# cable service class 5 activity-timeout 30
Router(config)# cable service class 5 admission-timeout 30

```

Configuring a Service Class for Peak-Rate

```

Router(config)# cable service class 201 name hsd
Router(config)# cable service class 201 downstream
Router(config)# cable service class 201 max-rate 1024000
Router(config)# cable service class 201 min-rate 1024000
Router(config)# cable service class 201 peak-rate 2000000

```

Command	Description
cable qos profile	Creates a DOCSIS 1.0 QoS profile.
show cable service-class	Displays the service classes that have been created.

cable service flow activity-timeout

To configure the activity timeout for dynamic cable service flows in DOCSIS 1.1 environments, where PacketCable is inactive, use the **cable service flow activity-timeout** command in global configuration mode. To remove the activity timer once configured, use the **no** form of this command.

cable service flow activity-timeout *n*

no cable service flow activity-timeout [*<n>*]

Syntax Description

n The timeout length in seconds. Valid range is 0 - 65535 seconds. Setting this value to 0 configures the service flow to never timeout.

Command Default

The default timeout length for a DOCSIS 1.0+ cable service flow is 300 seconds (five minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.3(13a)BC2	This command was introduced to support DOCSIS 1.1 service flow operation in non-Packet-Cable environments.

Usage Guidelines

Dynamic service flows in DOCSIS 1.0+ are created with a default activity timeout of 300 seconds. This enables the deletion of idle service flows after five minutes. This new command enables such functions within DOCSIS 1.1 environments with a wide range of timeout length options.

In DOCSIS 1.1, the default inactivity timeout is often set by the application that triggers the creation of dynamic service flows. PacketCable frequently performs this function when supported on the Cisco CMTS. However, this new command configures inactivity timeout where PacketCable is not active on the Cisco CMTS.



Note

When PacketCable is supported, PacketCable sets the inactivity timeout from the PacketCable gate, and the PacketCable activity overrides timeout values set with this command. This is the case even where the inactivity timeout is set to zero, which configures the service flow to never timeout.

Apart from PacketCable, this command enables the cable modem to control the setup of the dynamic service flows, and to remove inactive service flows. During the creation of service flows, all Upstream and Downstream flows in the request are checked to see if the configured activity timeout needs to be applied.



Note

The **cable service flow activity-timeout** command affects new calls only; it does not clear any existing hung flows. To clear existing flows, use the **test cable dsd <mac-add> <sid>** command.

Examples

The following example in global configuration mode configures the cable modems connected to the Cisco CMTS to use activity timeout of zero, which means that related service flows do not timeout in a non-PacketCable environment:

```
Router(config)# cable service flow activity-timeout 0
```

Related Commands

Command	Description
cable qos profile	Creates a DOCSIS 1.0 QoS profile.
cable service flow inactivity-threshold	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.1 operation).
cable service-flow inactivity-timeout	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.0 operation).
show cable service-class	Displays the service classes that have been created.

cable service flow inactivity-threshold

To set the inactivity threshold value for service flows using Unsolicited Grant Service with Activity Detection (UGS-AD), use the **cable service flow inactivity-threshold** command in global configuration mode. To disable the inactivity timer and reset the threshold limit timer to its default of 10 seconds, so that service flows revert to UGS activity only, use the **no** form of this command.

cable service flow inactivity-threshold *n*

no cable service flow inactivity-threshold *n*

Syntax Description

n Specifies the threshold limit in seconds, with 10 seconds as the default. Configurable limits are 1 to 3600 seconds.

Command Default

The default is to enable the inactivity timer, with a default value of 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)CX	This command replaced the cable service-flow inactivity-timeout command for DOCSIS 1.1 operation.
12.2(4)BC1	Support for this command was added to the Release 12.2 BC train.

Usage Guidelines

DOCSIS 1.1 allows a CM to request Unsolicited Grant Service (UGS) for an upstream, allowing the CM to reserve a certain amount of Constant Bit Rate (CBR) bandwidth for real-time traffic, such as Voice-over-IP (VoIP) calls. The UGS-AD variation allows the CMTS to switch a service flow to Real Time Polling Service (RTPS) after a certain period of inactivity, so that bandwidth is not reserved when it is not needed. The CM can then request UGS service when the flow again becomes active.



Note

This command replaced the **cable service-flow inactivity-timeout** command, which was used in DOCSIS 1.0 operation to enable or disable watchdog cleanup of dynamic service flows that are not sending any packets on the upstream.

The **cable service flow inactivity-threshold** command sets the inactivity timer for how long a service flow must be inactive before the CMTS can switch it from UGS-AD to RTPS. The **no cable service flow inactivity-threshold** command disables the timer and resets it to its default value of 10 seconds, so that the CMTS always provides UGS service to the service flow, even when the flow is idle.



Caution

The **no cable service flow inactivity-threshold** command effectively disables the use of RTPS and USG-AD services and configures the CMTS to provide only UGS services. This will prevent a CM that registered for USG-AD services from being able to obtain upstream transmission opportunities, resulting in a significant loss of bandwidth when a large number of CMs are requesting UGS-AD service flows.

Examples

The following example shows the inactivity timer being set to 20 seconds:

```
Router(config)# cable service flow inactivity-threshold 20
Router(config)#
```

The following command disables the inactivity timer, so that the service flow remains UGS, even during periods of inactivity:

```
Router(config)# no cable service flow inactivity-threshold
Router(config)#
```

Related Commands

Command	Description
cable service class	Sets the DOCSIS 1.1 service class parameters.
cable service-flow inactivity-timeout	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.0 operation).
show controllers cable	Displays information for the cable interface.

cable service-flow inactivity-timeout

To set the amount of time a dynamic service-flow can be present in the system without any activity, use the **cable service-flow inactivity-timeout** command in global configuration mode. To remove the specification, use the **no** form of this command.

cable service-flow inactivity-timeout *minutes*

no cable service-flow inactivity-timeout

Syntax Description

minutes Specifies service-flow inactivity-timeout in minutes. Valid range is 1 to 120 minutes. Default value is 30 minutes.

Command Default

30 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(3a)EC	This command was introduced.
12.1(4)CX	This command was replaced by the cable service flow inactivity-threshold command for DOCSIS 1.1 operation.

Usage Guidelines

Resources such as service identifiers (SIDs) and bandwidth are dynamically allocated by a CM using Dynamic Service Addition (DSA) transaction. If the CM fails to release these resources by issuing a Dynamic Service Deletion (DSD), then the resources might be locked indefinitely. Use this command to release unused resources.

Examples

The following example shows how to set the inactivity timeout for dynamic service flows to 2 minutes. Once this setting is specified, any dynamic SID that does not show any activity in 2 minutes will be deleted.

```
Router(config)# cable service-flow inactivity-timeout 2
```

The following example shows how to set the inactivity timeout back to the default value of 30 minutes:

```
Router(config)# cable service-flow inactivity-timeout
```

Related Commands

Command	Description
cable service flow inactivity-threshold	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.1 operation).
cable qos permission	Specifies permission for updating the cable router QoS table.

Command	Description
cable qos profile	Configures a QoS profile.
show controllers cable	Displays QoS profiles.

cable service type

To redirect CMs matching a service-type to downstream frequency, use the **cable service type** command in global configuration mode. To cancel the redirection of CMs, use the **no** form of this command.

cable service type *service-type-id* **ds-frequency** *frequency*

no cable service type *service-type-id* **ds-frequency** *frequency*

Syntax Description

service-type-id Specifies the service type identifier to be redirected.
The maximum length of *service-type-id* is 16.

ds-frequency *frequency* Specifies the downstream frequency the CMs will be redirected to.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command will redirect the CMs matching a particular service-type identifier to downstream frequency. Multiple service types can be redirected to one frequency. However, one service type cannot be redirected to multiple DS frequencies.

Examples

The following example shows how to redirect the CMs matching the service type to downstream frequency:

```
Router(config)# cable service type commercial ds-frequency 519000000
```

cable sflog

To enable service flow logging and to configure the number and duration of entries in the log, use the **cable sflog** command in global configuration mode. To disable service flow logging, use the **no** form of the command.

cable sflog max-entry *number* **entry-duration** *time*

no cable sflog

Syntax Description

max-entry <i>number</i>	Specifies the maximum number of entries in the service flow log. When the log becomes full, the oldest entries are deleted to make room for new entries. The valid range is 0 to 59999, with a default of 0 (which disables service flow logging).
Note	The max-entry value applies to the entire chassis on the Cisco uBR7100 series and Cisco uBR7200 series routers, but applies to individual cable line cards on the Cisco uBR10012 router.
entry-duration <i>time</i>	Specifies how long, in seconds, entries can remain in the service flow log. The CMTS deletes entries in the log that are older than this value. The valid range is 1 to 86400 seconds, with a default value of 3600 seconds (1 hour).

Defaults

max-entry = 0 (service flow logging is disabled) and **entry-duration** = 3600 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)BC1	This command was introduced.

Usage Guidelines

A DOCSIS specification currently being developed requires the DOCSIS CMTS to maintain a log table that contains entries of deleted service flows. The **cable sflog** command enables the logging of deleted service flows in this table and also sets the maximum number of entries in the log. When the log becomes full, the oldest entries are deleted to make room for the newest ones.

This command also configures how long each entry can remain in the log. When an entry has been in the table for the specified time, the CMTS deletes it, even if the log is not currently full.

To display the service flow log, use SNMP commands to display the docsQosServiceFlowLogEntry entries in the docsQosServiceFlowLogTable table. These attributes are defined in the *Data Over Cable System Interface Specification Quality of Service Management Information Base (DOCSIS-QOS MIB)* internet draft.

Cisco IOS Release 12.2(15)BC1 supports version 4 of this DOCSIS-QOS MIB draft, which is available on the IETF Internet-Drafts web site:

<http://http://www.ietf.org/ID.html>

**Note**

At the time of this document's release, the DOCSIS-QOS MIB is still in draft form and is therefore subject to change in future releases of Cisco IOS software.

The **max-entry** value specified by this command applies to the entire chassis for the Cisco uBR7100 series and Cisco uBR7200 series routers, but to individual line cards on the Cisco uBR10012 router. However, the Cisco uBR10012 router still maintains only one log table for all deleted service flows.

For example, if the **max-entry** value is set to 10,000 on a Cisco uBR7200 series router, the service flow log table holds a maximum of 10,000 entries for all cable line cards in the chassis. If the **max-entry** value is set to 10,000 on a Cisco uBR10012 router that has four cable line cards installed, the service flow log table holds a maximum of 40,000 entries, with each cable line card having a maximum of 10,000 entries each.

Examples

The following example shows how to enable service flow logging with a maximum of 2,000 entries in the log, and with each entry remaining in the log for a maximum of 2 hours (7200 seconds):

```
Router(config)# cable sflog max-entry 2000 entry-duration 7200
```

The following example shows how to set the **max-entry** value to its default of 0 and disable service flow logging:

```
Router# configure terminal
Router(config)# no cable sflog
Router(config)# exit
Router#
```

Related Commands

Command	Description
cable service-flow inactivity-timeout	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.0 operation).
cable service flow inactivity-threshold	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.1 operation).

cable shared-secondary-secret

To configure one or more secondary shared-secret keys that CMTS can use to successfully process the DOCSIS configuration file and register with the CMTS, use the **cable shared-secondary-secret** command in cable interface configuration mode. To remove the secondary shared secrets, use the **no** form of this command.

cable shared-secondary secret index *index-num* [0 | 7] *authentication-key*

no cable shared-secondary secret index *index-num*

Syntax Description	index <i>index-num</i>	Specifies the order in which the CMTS will use the secondary shared-secrets to verify the CM during the registration process. The valid range is 1 to 16.
	0	(Optional) Specifies that an unencrypted message will follow.
	7	(Optional) Specifies that an encrypted message will follow.
		Note As a general rule, the 7 option is not used by users at the command line because it requires a pre-encrypted password. Typically, the 7 option is useful only when cutting and pasting commands from another router's configuration file.
	<i>authentication-key</i>	Text string specifying the shared secret string. When you also use the service password-encryption command, the key is stored in encrypted form. The text string can be any arbitrary string up to 80 characters in length.

Defaults

No secondary shared secret is used. If no encryption option is specified, the key is stored in the configuration file as encrypted text if the **service password-encryption** command has also been given.

Command Modes

Interface configuration (cable interface only)

Command History

Release	Modification
12.2(8)BC2	This command was introduced.

Usage Guidelines

The **cable shared-secondary-secret** command can be used to supplement the **cable shared-secret** command so as to prevent unauthorized interception and alteration of the DOCSIS configuration file that is downloaded to the CM during the registration process. The DOCSIS specification allows for a CM and CMTS to use a shared secret (a secret encryption string) to calculate the MD5 Message Integrity Check (MIC) value for the DOCSIS configuration file that is downloaded to the CM.

The CM must use the proper shared secret encryption string to successfully decrypt and process the configuration file, and then register with the CMTS. If the CM does not have the proper encryption string, it will be unable to calculate the proper MIC value, and the **show cable modem** command will show **reject(m)** for the modem to indicate a MIC authentication failure.

The **cable shared-secondary-secret** command allows a cable operator to specify up to 16 alternate DOCSIS shared secrets. If a CM has a MIC authentication failure during registration, the CMTS then checks the MIC values using the alternate shared secrets. If a match is found, the CM is allowed online. If none of the alternate MIC values match the value returned by the CM, the CMTS refuses to allow the CM to come online and instead logs a MIC authentication failure.

The use of secondary shared secrets allow the MSO to gradually phase in changes to the shared secret key. If a shared secret has been compromised, or if the MSO decides to regularly change the shared secret, the MSO can use the **cable shared-secret** command to immediately change the primary shared secret. The previous key can then be made a secondary shared secret, using the **cable shared-secondary-secret** command, so that CMs can continue to register until the MSO can change all of the DOCSIS configuration files to use the new shared secret.

To use the secondary shared-secret feature, you must do the following:

- You must specify a shared secret with the **cable shared-secret** command. The **cable shared-secondary-secret** command has no effect if you have not specified a primary shared secret.

**Note**

At any particular time, the majority of CMs should use the primary shared secret to avoid excessive registration times.

- Create DOCSIS configuration files that use the shared-secret encryption string to create the MD5 MIC value. This can be done using the Cisco DOCSIS Configurator tool by entering the shared-secret string in the **CMTS Authentication** field in the **Miscellaneous** parameters.

**Tip**

The shared-secret string itself is not saved in the DOCSIS configuration file, so you must re-enter the string in the **CMTS Authentication** field whenever you create or edit a DOCSIS configuration file using the Cisco DOCSIS Configurator tool.

- Use the **cable shared-secondary-secret** command to configure the cable interfaces with one or more matching shared-secret strings. The string configured on an interface must match the string used to create the DOCSIS configuration files downloaded to the CMs on that interface, or the CMs will not be able to register. You can use different shared secrets for each interface, if you are also using a different set of configuration files for each interface.
- To encrypt the shared-secret strings in the CMTS configuration, you must include the **service password-encryption** global configuration command in the router's configuration.

**Note**

You cannot use the shared secret feature with the files created by the internal DOCSIS configuration file editor (**cable config-file** command).

Examples

The following example shows how to specify multiple secondary shared-secret string using encrypted keys:

```
Router# config t
Router(config)# service password-encryption
Router(config)# int c6/0
Router(config-if)# cable shared-secret n01jk_1a
Router(config-if)# cable shared-secondary-secret index 1 cabl3-x21b
Router(config-if)# cable shared-secondary-secret index 2 dasc9_ruld55ist5q3z
Router(config-if)# cable shared-secondary-secret index 3 j35u556_x_0
Router(config-if)# exit
```

```

Router(config)# exit
Router# show running-config | include shared
cable shared-secret 7 1407513181A0F13253920
cable shared-secondary-secret 7 14031A021F0D39263D3832263104080407
cable shared-secondary-secret 7 071B29455D000A0B18060615142B38373F3C2726111202431259545D6
cable shared-secondary-secret 7 0501555A34191B5F261D28420A555D
Router#

```

**Note**

In this example, the shared-secret strings are initially entered as clear text, but because the **service password-encryption** command has been used, the strings are encrypted in the configuration file.

Related Commands

Command	Description
cable dynamic-secret	Enables the dynamic shared secret feature, so that DOCSIS configuration files are verified with a dynamically generated shared secret.
cable shared-secret	Configures an authentication shared-secret key that CMs must use to successfully process the DOCSIS configuration file and register with the CMTS.
cable tftp-enforce	Requires that all CMs on a cable interface attempt to download a DOCSIS configuration file using the Trivial File Transfer Protocol (TFTP) through the cable interface before being allowed to register and come online.

cable shared-secret

To configure an authentication shared-secret encryption key that CMs must use to successfully process the DOCSIS configuration file and register with the CMTS, use the **cable shared-secret** command in cable interface configuration mode. To disable the use of a shared-secret key during the CM registration phase, use the **no** form of this command.

cable shared-secret [**0** | **7**] *authentication-key*

no cable shared-secret

Syntax Description		
	0	(Optional) Specifies that an unencrypted message (clear text) will follow.
	7	(Optional) Specifies that an encrypted message will follow.
		Note As a general rule, the 7 option is not used by users at the command line because it requires a pre-encrypted password. Typically, the 7 option is useful only when cutting and pasting commands from another router's configuration file.
	<i>authentication-key</i>	Text string specifying the shared secret string. When you also use the service password-encryption command, the key is stored in encrypted form. The text string can be any arbitrary string up to 80 characters in length.

Defaults

No shared-secret encryption key is used during registration, only the default DOCSIS MD5-encrypted checksum. When **cable shared-secret** is given without specifying an encryption option, the key is stored in the configuration file as an encrypted password if the **service password-encryption** command has also been given.

Command Modes

Interface configuration (cable interface only)

Command History

Release	Modification
11.3 XA	This command was introduced.

Usage Guidelines

The **cable shared-secret** command can be used to prevent unauthorized interception and alteration of the DOCSIS configuration file that is downloaded to the CM during the registration process. The **cable shared-secret** command specifies a secret encryption string that the CMTS uses to calculate the MD5 Message Integrity Check (MIC) value that is appended to every DOCSIS configuration file and that the CM and CMTS use to verify the file's integrity.

The CM must use the shared secret encryption string to successfully decrypt and process the configuration file, and then register with the CMTS. If the CM does not have the proper encryption string, it will be unable to calculate the proper MIC value, and the **show cable modem** command will show **reject(m)** for the modem to indicate a MIC authentication failure.

To use the shared-secret feature, you must do the following:

- Create DOCSIS configuration files that use the shared-secret encryption string to create the MD5 MIC value. This can be done using the Cisco DOCSIS Configurator tool by entering the shared-secret string in the **CMTS Authentication** field in the **Miscellaneous** parameters.



Note The shared-secret string itself is not saved in the DOCSIS configuration file, so you must re-enter the string in the **CMTS Authentication** field whenever you create or edit a DOCSIS configuration file using the Cisco DOCSIS Configurator tool.

- Use the **cable shared-secret** command to configure the cable interfaces with a matching shared-secret string. The string configured on an interface must match the string used to create the DOCSIS configuration files downloaded to the CMs on that interface, or the CMs will not be able to register. You can use different shared secrets for each interface, if you are also using a different set of configuration files for each interface.
- To encrypt the shared-secret string in the CMTS configuration, you must include the **service password-encryption** global configuration command in the router's configuration.



Note You cannot use the shared secret feature with the files created by the internal DOCSIS configuration file editor (**cable config-file** command).



Note In Cisco IOS Release 12.2(8)BC2 and later releases, you can also use the **cable shared-secondary-secret** command to specify multiple shared-secret strings, so that you can gradually phase in a new shared secret string.

Upgrading When Using Shared Secret Passwords

Cisco IOS Release 12.2 BC changed the encryption algorithm used for the **cable shared-secret** command. If you are upgrading from a Cisco IOS 12.1 EC or 12.0 SC release, you cannot cut and paste the **cable shared-secret** configuration lines that include an encrypted password. Instead, you must re-enter the original shared secret passwords at the CLI prompt, and then resave the configuration.

For example, if the actual shared secret password is “cm-sharedsecret-password”, enter the **cable shared-secret cm-sharedsecret-password** command at the CLI prompt. If you have enabled password encryption, the configuration file will then show only the newly encrypted password.



Note This change affects only the encryption of the passwords that are stored in the configuration file. It does not affect the actual encryption that is used between the CMTS and CMs, so you do not need to change the shared secret in the DOCSIS configuration files for the CMs.

Examples

The following example shows how to specify a shared-secret string using an encrypted key:

```
Router# config t
Router(config)# service password-encryption
Router(config)# int c6/0
Router(config-if)# cable shared-secret password
Router(config-if)# exit
Router(config)# exit
Router# show running-config | include shared
cable shared-secret 7 1407513181A0F13253920
```

**Note**

Router#

In this example, the shared-secret string is initially entered as clear text, but because the **service password-encryption** command has been used, the string is encrypted in the configuration file.

The following example shows how to remove the use of a shared-secret encryption key on a cable interface. That particular interface then ignores any shared-secret that is used when calculating the MD5 checksum:

```
Router# config t
Router(config)# int c6/0
Router(config-if)# no cable shared-secret
Router(config-if)# end
Router#
```

Related Commands

Command	Description
cable dynamic-secret	Enables the dynamic shared secret feature, so that DOCSIS configuration files are verified with a dynamically generated shared secret.
cable shared-secondary-secret	Configures one or more secondary shared-secret keys that CMs can use to successfully process the DOCSIS configuration file and register with the CMTS.
cable tftp-enforce	Requires that all CMs on a cable interface attempt to download a DOCSIS configuration file using the Trivial File Transfer Protocol (TFTP) through the cable interface before being allowed to register and come online.

cable source-verify

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

cable source-verify [**dhcp** | **leasetimer** *value*]

no cable source-verify

Syntax Description	
dhcp	(Optional) Specifies that queries will be sent to verify unknown source IP addresses in upstream data packets. Note Do not enable the local DHCP server on the Cisco CMTS and configure local DHCP address pools, using the ip dhcp pool command, when using this option, because this prevents DHCP address validation.
leasetimer <i>value</i>	(Optional) Specifies the time, in minutes, for how often the router should check its internal CPE database for IP addresses whose lease times have expired. The valid range for value is 1 to 240 minutes, with a default of 60 minutes. Note The leasetimer option takes effect only when the dhcp option is also used on an interface. Also, this option is supported only on the master interface and cannot be configured on subinterfaces. Configuring it for a master interface automatically applies it to all subinterfaces.

Command Default Disabled. When the **dhcp** option is specified, the **leasetimer** option defaults to 60 minutes.

Command Modes Cable interface and subinterface configuration



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

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

Release	Modification
12.2(15)BC2	Support for verifying CMs and CPE devices that are on a different subnet than the cable interface was enhanced to use Reverse Path Forwarding (RFP).
12.3(9a)BC	Cisco IOS Release 12.3(9a)BC adds the option of using a per SID basis for deriving lease queries from CPE devices. This release also introduces a global rate limit for lease queries initiated by downstream traffic.

Usage Guidelines

The **cable source-verify** command helps to prevent the spoofing of IP addresses by CMs or their CPE devices by verifying that the upstream packets coming from each CM are known to be associated with the IP address in that packet. Packets with IP addresses that do not match those associated with the CM are dropped.

In order to protect the Cisco CMTS from denial of service attacks, Cisco IOS Release 12.3(9a)BC adds the option of using a per SID basis for deriving lease queries from CPE devices. This release also introduces a global rate limit for lease queries initiated by downstream traffic. These enhancements reduce the CPU utilization of DHCP Receive and ISR processes when the Cisco CMTS is configured with the **cable source-verify dhcp** and **no cable arp** commands.



Caution

In current Cisco IOS Release 12.1 EC and 12.2 BC software images, the Cisco CMTS can crash with a “bus error exception” when the **cable source-verify** command is configured on a cable interface, and the routing configuration of that interface is being changed while traffic is passing through the interface. To avoid this problem, temporarily disable this feature (using **no cable source-verify**) on the interface before you configure the routing parameters. Then after you have finished the routing configuration, reenables the feature using the **cable source-verify** command. Alternatively, you can also change the routing parameters when the interface is not passing traffic (such as when the interface is shut down).



Caution

In Cisco IOS Release 12.2(15)BC1 and earlier releases, you cannot use the **cable source-verify** command on a Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, or Cisco uBR-MC5X20S/U cable interface line card that is using an MPLS/VPN configuration when you are also using duplicate or overlapping IP address ranges for CPE devices on different cable interfaces/subinterfaces. To use the **cable source-verify** command, you must assign unique IP addresses for each cable interface or sub-interface. This is being tracked as caveat CSCed53355.

The Cisco CMTS maintains a database that links the MAC and IP addresses of known CPE devices with the CMs that are providing network access for those CPE devices. The CMTS typically populates this database with information obtained by examining the Dynamic Host Configuration Protocol (DHCP) packets sent between the CPE devices and the DHCP server. Other IP traffic provides information about which CMs service which CPE devices.

After the **cable source-verify** command is issued, every IP upstream packet is examined. If the IP and MAC addresses of the CPE device are already associated with a known, online CM, it is allowed through. If not, the source IP address is examined to determine if it belongs to the cable network. If so, and if the **dhcp** option is not used, the packet is allowed through.

Using the dhcp Option

If the **dhcp** option is used, all packets with unknown IP addresses within the cable network are dropped, but the Cisco CMTS sends a DHCP LEASEQUERY message to the DHCP server to verify the IP address. If a valid response is received from the DHCP server, the 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.

In Cisco IOS Release 12.2(15)BC1 and later releases, the **dhcp** option extends the verification to CPE devices that had been online using a valid IP address but then were reconfigured by the user with an unused static IP address. With Cisco IOS Release 12.2(15)BC1 and later, CPE devices are not allowed online when they are using static IP addresses that have not been allocated by the DHCP server. If you are using the **dhcp** option, the CPE device must use an IP address that has been assigned by the DHCP server.



Note

The **dhcp** option automatically blocks all statically-assigned IP addresses unless the DHCP server has been configured to recognize those addresses and respond with the appropriate LEASEQUERY response.

The **cable source-verify** command by itself prevents someone from stealing another customer's IP address. The **cable source-verify dhcp** command adds another level of security by refusing access to any CPE device with an IP address that has not been assigned by the DHCP server.



Note

This **dhcp** option requires that the DHCP server support the LEASEQUERY message. The Cisco Network Registrar (CNR) supports LEASEQUERY in version 3.01(T) and above. The LEASEQUERY message is currently defined in an IETF draft, which is dated October, 2003 and available at the following URL:

<http://www.ietf.org/internet-drafts/draft-ietf-dhc-leasequery-06.txt>



Caution

Do not enable the local DHCP server on the Cisco CMTS and configure local DHCP address pools, using the **ip dhcp pool** command, when you are also enabling the **cable source-verify dhcp** command, because the DHCP server on the Cisco CMTS can intercept the LEASEQUERY messages and prevent them from reaching the external DHCP server. This in turn prevents address validation from succeeding because the DHCP server on the Cisco CMTS does not support LEASEQUERY messages.



Note

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

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 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.

**Note**

The **leasetimer** option is active only if you have also specified the **cable source-verify dhcp** command for the cable interface. If the **dhcp** option is not used, the leasetimer option has no effect. In addition, the **leasetimer** option can be configured only on an interface, not a subinterface. Applying it to a master interface automatically applies it to all subinterfaces.

The **leasetimer** option allows you to configure how often the timer checks the lease times, so as to specify the maximum amount of time a CPE device can use an IP address that was previously assigned by the DHCP server but whose lease time has since expired. The time period can range from 1 minute to 240 minutes (4 hours), with a grace period of 2 minutes to allow a PC enough time to make a DHCP request to renew the IP address. To turn off the timer, so that the CMTS no longer checks the lease times, issue the **cable source-verify** command without the **dhcp** option, or turn off the feature entirely with the **no cable source-verify** command.

Using Multiple Subnets

In Cisco IOS Release 12.2(15)BC2 and later releases, the **cable source-verify** command can verify IP addresses that are on a different subnet than what is being used on the cable interface only if you also enable Reverse Path Forwarding (RPF) checks by configuring the following commands:

```
Router(config)# ip cef
Router(config)# interface cable interface
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)#
```

Examples

The following example shows how to turn on CM upstream verification and configures the Cisco CMTS router to send DHCP LEASEQUERIES to verify unknown source IP addresses in upstream data packets:

```
Router# configure terminal
Router#(config) interface c4/0
Router(config-if)# cable source-verify dhcp
Router(config-if)#
```

The following example shows how to enable the **leasetimer** feature so that every two hours, the CMTS checks the IP addresses in the CPE database for that particular interface for expired lease times:

```
Router# configure terminal
Router#(config) interface c1/0
Router(config-if)# cable source-verify dhcp
Router(config-if)# cable source-verify leasetimer 120
Router(config-if)#
```

The following example shows how to configure the cable interface so that the CMTS can verify IP addresses that are on a different subnet than the one that the cable interface is using:

```
Router# configure terminal
Router(config)# ip cef
Router#(config) interface c7/0/0
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# cable source-verify dhcp
Router(config-if)#
```

The following example shows the error message that is displayed if you try to configure the **leasetimer** option on a subinterface, instead of an interface:

```

Router# configure terminal
Router#(config) interface c1/0.1
Router(config-subif)# cable source-verify dhcp
Router(config-subif)# cable source-verify leasetimer 120
% Invalid input detected at '^' marker.

Router(config-subif)#

```

Related Commands

Command	Description
cable arp	Enables or disables the use of the ARP protocol for CMs and their CPE devices.
cable helper-address	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast (DHCP) packets.
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 logging badipsource	Logs error messages about bad IP source addresses on the cable interfaces.
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 leasequery-filter downstream	Controls the number of DHCP LEASEQUERY request messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco CMTS router.
cable source-verify leasequery-filter upstream	Controls the number of DHCP LEASEQUERY request messages that are sent for unknown IP addresses per each service ID (SID) on an upstream.
clear cable logging	Removes all error messages about bad IP source addresses on the cable interfaces from the error log buffer.
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.
ip verify unicast reverse-path	Enables Unicast Reverse Path Forwarding (Unicast RPF), which checks each packet received on an interface to verify that the packet's source IP address appears in the routing tables as belonging to that interface, so as to prevent spoofed IP source addresses.

cable source-verify leasequery-filter downstream

To control the number of Dynamic Host Configuration Protocol (DHCP) LEASEQUERY request messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco Cable Modem Termination System (CMTS) router, use the **cable source-verify leasequery-filter downstream** command in global configuration mode. To stop the filtering of DHCP lease queries, use the **no** form of this command.

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

no cable source-verify leasequery-filter downstream

Syntax Description

<i>threshold</i>	Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 255 lease queries.
<i>interval</i>	Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 10 seconds.

Command Default

Filtering of DHCP lease queries is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)BC1d, 12.2(15)BC2b	This command was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers.

Usage Guidelines

When the **cable source-verify dhcp** and **no cable arp** commands are configured on a cable interface, the Cisco CMTS router sends a DHCP LEASEQUERY request to the DHCP server to verify unknown IP addresses that are found in packets to and from customer premises equipment (CPE) devices that are using the cable modems on the cable interface. The DHCP server returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any. The router can then verify that this CPE device is authorized to use this IP address, which prevents users from assigning unauthorized IP addresses to their CPE devices.

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks scan ranges of IP addresses, in an attempt to find unused addresses. This type of activity can generate a large volume of DHCP LEASEQUERY requests, which can result in high CPU utilization and a lack of available bandwidth for other customers.

To prevent such a large volume of LEASEQUERY requests on all downstreams in the Cisco CMTS router, use the **cable source-verify leasequery-filter downstream** command. After configuring this command, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests in the downstream direction within each interval time period.

For example, the **cable source-verify leasequery-filter downstream 5 10** command configures the router so that it allows a maximum of 5 DHCP LEASEQUERY requests every 10 seconds for each SID on the downstream direction. This command applies to all downstream cable interfaces in the router.

**Note**

The **cable source-verify leasequery-filter downstream** command enables DHCP lease query filtering on all downstreams, but the actual filtering does not begin until the **cable source-verify dhcp** command and the **no cable arp** command are configured on a particular downstream. You can configure these commands on either the downstream's main interface, or on a subinterface for the downstream. If these commands are configured on a subinterface, however, the lease query filtering occurs only for cable modems using that subinterface.

**Tip**

Use the **cable source-verify leasequery-filter upstream** command to filter DHCP LEASEQUERY requests in the upstream direction.

Examples

The following example shows how to configure the Cisco CMTS router so that it allows a maximum of 10 DHCP lease query requests per SID over each five-second interval on all downstream cable interfaces. This example also shows the configuration of **cable source-verify dhcp** and **no cable arp** commands on a cable interface, which are required to use this feature.

```
Router# configure terminal
Router(config)# cable source-verify leasequery-filter downstream 10 5
Router(config)# interface cable 5/1/0
Router(config-if)# cable source-verify dhcp
Router(config-if)# no cable arp
Router(config-if)#
```

Related Commands

Command	Description
cable arp	Activates the cable Address Resolution Protocol (ARP).
cable arp filter	Controls the number of ARP requests and replies that can be forwarded over a cable interface.
cable source-verify	Enables verification of IP addresses for cable modems (CMs) and CPE devices on the upstream.
cable source-verify leasequery-filter upstream	Controls the number of DHCP lease query messages that are sent for unknown IP addresses per each service ID (SID) on an upstream.
show cable leasequery-filter	Displays the number of DHCP lease query messages that have been filtered for all cable modems or for a particular cable interface.

cable source-verify leasequery-filter upstream

To control the number of Dynamic Host Configuration Protocol (DHCP) LEASEQUERY request messages that are sent for unknown IP addresses per each service ID (SID) on an upstream, use the **cable source-verify leasequery-filter upstream** command in cable interface configuration mode. To disable the filtering of DHCP lease queries, use the **no** form of this command.

cable source-verify leasequery-filter upstream *threshold interval*

no cable source-verify leasequery-filter upstream

Syntax Description		
<i>threshold</i>		Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 20 lease queries.
<i>interval</i>		Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 5 seconds.

Defaults Filtering of DHCP lease queries is disabled.

Command Modes Interface configuration (cable interface only)

Command History	Release	Modification
	12.2(15)BC1d, 12.2(15)BC2b	This command was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers.

Usage Guidelines When the **cable source-verify dhcp** and **no cable arp** commands are configured on a cable interface, the Cisco Cable Modem Termination System (CMTS) router sends a DHCP LEASEQUERY request to the DHCP server to verify unknown IP addresses that are found in packets to and from customer premises equipment (CPE) devices that are using the cable modems on the cable interface. The DHCP server returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any. The router can then verify that this CPE device is authorized to use this IP address, which prevents users from assigning unauthorized IP addresses to their CPE devices.

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks scan ranges of IP addresses, in an attempt to find unused addresses. This type of activity can generate a large volume of DHCP LEASEQUERY requests, which can result in high CPU utilization and a lack of available bandwidth for other customers.

To prevent such a large volume of LEASEQUERY requests on the upstreams on a cable interface, use the **cable source-verify leasequery-filter upstream** command. After configuring this command, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests in the upstream direction within each interval time period.

For example, the **cable source-verify leasequery-filter upstream 5 5** command configures the router so that it allows a maximum of 5 DHCP LEASEQUERY requests every 5 seconds for each SID on the upstream direction. This command applies to all upstreams on the cable interface.

**Note**

The **cable source-verify leasequery-filter upstream** command enables DHCP lease query filtering on all upstreams on a cable interface, but the actual filtering does not begin until the **cable source-verify dhcp** command and the **no cable arp** command are configured on the upstream's associated downstream interface. You can configure these commands on either the downstream's main interface, or on a subinterface for the downstream. If these commands are configured on a subinterface, however, the lease query filtering occurs only for cable modems using that subinterface.

**Note**

If using cable interface bundling, configure the **cable source-verify leasequery-filter upstream** command on all master and slave interfaces.

**Tip**

Use the **cable source-verify leasequery-filter downstream** command to filter DHCP LEASEQUERY requests in the downstream direction.

Examples

The following example shows how to configure the Cisco CMTS router so that it allows a maximum of five DHCP lease query requests per SID over each two-second interval on all upstreams on a particular cable interface. This example also shows the configuration of **cable source-verify dhcp** and **no cable arp** commands on the cable interface, which are required to use this feature.

```
Router# configure terminal
Router(config)# interface cable 6/0
Router(config-if)# cable source-verify dhcp
Router(config-if)# cable source-verify leasequery-filter upstream 5 2
Router(config-if)# no cable arp
Router(config-if)#
```

Related Commands

Command	Description
cable arp	Activates the cable Address Resolution Protocol (ARP).
cable arp filter	Controls the number of ARP requests and replies that can be forwarded over a cable interface.
cable source-verify	Enables verification of IP addresses for cable modems (CMs) and CPE devices on the upstream.
cable source-verify leasequery-filter downstream	Controls the number of DHCP lease query messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco CMTS router.
show cable leasequery-filter	Displays the number of DHCP lease query messages that have been filtered for all cable modems or for a particular cable interface.

cable spectrum-group (global)

To create and configure a spectrum group, use the **cable spectrum-group** command in global configuration mode. To disable this spectrum group, use the **no** form of this command.

cable spectrum-group *group-number* [**time** *day hh:mm:ss*] **frequency** *up-freq-hz* [*pwr-lvl-dbmV*]

cable spectrum-group *group-number* [**time** *day hh:mm:ss*] **band** *up-freq1-hz up-freq2-hz* [*pwr-lvl-dbmV*]

no cable spectrum-group *group-number*

Syntax Description

<i>group-number</i>	Specifies the spectrum group for which you are specifying a parameter value or specifies the number of the spectrum group you wish to remove from your router configuration. Valid range is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.
time <i>day hh:mm:ss</i>	(Optional) for scheduled spectrum groups, enter the day of the week (Sun—Sat) and the time of day that the frequency and input power level should change.
frequency <i>up-freq-hz</i>	Specifies a center frequency for the upstream group. The valid range is 5,000,000 Hz to 42,000,000 Hz (DOCSIS), 55,000,000 Hz (Japan), or 65,000,000 (EuroDOCSIS). Note You can enter this command multiple times for the same spectrum group to create a group of individual frequencies to be used for frequency hopping.
band <i>up-freq1-hz up-freq2-hz</i>	Specifies a range of center frequencies the Cisco CMTS can scan to find an acceptable channel to which the spectrum group may hop. The valid range for <i>up-freq1-hz</i> is 5,000,000 Hz to 42,000,000 Hz (DOCSIS), 55,000,000 Hz (Japan), or 65,000,000 (EuroDOCSIS), but <i>up-freq2-hz</i> must be greater than <i>up-freq1-hz</i> . Note When creating spectrum groups for cable line cards that support Advanced Spectrum Management (Cisco uBR10-MC16S, uBR10-MC16U/X, uBR10-MC28U/X, and uBR10-MC5X20S/U), use the band option. The frequency option is not supported for these types of line cards.
<i>pwr-lvl-dbmV</i>	(Optional) Specifies the nominal input power level. The valid range is -10 to +25 dBmV, with a default of 0 dBmV. Some cable plants might want to change only the input power level, and not the frequency, on a daily time schedule.

Command Default

If not specified, the group is set for a nominal input power level of 0 dBmV and the group is not scheduled for automatic frequency or power changes.

Command Modes

Global configuration

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(7)XR2	The band parameter for this command was added to enable frequency range scanning capabilities in the Cisco uBR-MC16S cable interface line card.
12.0(13)SC, 12.1(4)EC, 12.2(4)BC1	The allowable frequency range was increased to 65 MHz to support the EuroDOCSIS frequency range of the Cisco uBR-MC16E cable interface line card.
12.2(15)BC2	The maximum number of spectrum groups was increased from 32 to 40 groups per router.

Usage Guidelines

Frequency agility is configured and activated using spectrum groups that are controlled by the spectrum manager. You can create from 1 to 32, or from 1 to 40, spectrum groups for each cable modem card upstream port, depending on the Cisco IOS software release.

To create spectrum groups, specify a list of upstream frequencies and nominal power levels that each spectrum group can use when an upstream frequency change is necessary. Each spectrum group should have its own list of upstream frequencies. At 1.6 MHz, the valid range is -10 dBmV to 25 dBmV. The power level value should be changed only if you want to change only the power level as part of spectrum management. The standard power level is 0 dBmV.

The **cable spectrum-group** command sets the center frequency for the upstream, but the total frequency bandwidth that is actually used depends on the channel width. [Table 0-11](#) shows the possible center frequencies for each channel width, for both DOCSIS and EuroDOCSIS cable interfaces.

Table 0-11 Allowable Center Frequencies

Channel Width (MHz)	Center Frequency (MHz) DOCSIS (5 to 42 MHz)	Center Frequency (MHz) EuroDOCSIS (5 to 65 MHz)
200,000	5.1 to 41.9	5.1 to 64.9
400,000	5.2 to 41.8	5.2 to 64.8
800,000	5.4 to 41.6	5.4 to 64.6
1,600,000	5.8 to 41.2	5.8 to 64.2
3,200,000	6.6 to 40.4	6.6 to 63.4

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 0-12 Allowable Frequency Range for the cable upstream frequency Command

Frequency Range	Supported Cable Interfaces	Minimum Cisco IOS Releases
5 to 42 MHz	All supported cable interfaces	All releases supported for the Cisco CMTS

Table 0-12 Allowable Frequency Range for the cable upstream frequency Command

Frequency Range	Supported Cable Interfaces	Minimum Cisco IOS Releases
5 to 55 MHz	Cisco uBR-MC16U/X and Cisco uBR-MC28U/X, when operating with extended frequencies for Japanese mode	Cisco IOS Release 12.2(15)BC2
5 to 65 MHz	Cisco uBR-MC16E, Cisco uBR7111E and Cisco uBR7114E routers	Cisco IOS Release 12.0(13)SC, 12.1(4)EC, and 12.2(4)BC1

**Note**

If both an Cisco uBR-MC16E cable interface line card and a Cisco uBR-MC16C or a Cisco uBR-MC16S cable interface line card are present in the chassis, a spectrum group in the 42-MHz to 65-MHz range should not be assigned.

**Tip**

Cisco cable interface line cards always program the upstream's center frequency in 16 KHz increments, and this is the frequency displayed by the **show controller cable upstream** command. For example, if you use the **cable upstream frequency** command to specify a center frequency of 27 MHz (**cable upstream x frequency 27000000**), the actual center frequency will be 27.008 MHz, which is the next highest 16 KHz boundary.

You must repeat this command for each frequency or power level that you want to add to a spectrum group's list of valid values.

After you have created one or more spectrum groups for your cable network, you can add characteristics to them, providing you with more definitive control over frequency usage and frequency hopping.

The cable interface does not operate until you either create and configure a spectrum group or set a fixed upstream frequency. See the **cable upstream channel-width** command.

Examples

The following example shows how to configure spectrum group 1 with an upstream frequency of 6,500,000 Hz and a default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 1 frequency 6500000
```

The following example shows how to add the upstream frequency 7,000,000 Hz to the list of valid frequencies with a default power level of 0 dBmV for spectrum group 1:

```
Router(config)# cable spectrum-group 1 frequency 7000000
```

The following example shows how to configure spectrum group 2 with an upstream frequency 7,500,000 Hz and change the power level to 5 dBmV:

```
Router(config)# cable spectrum-group 2 frequency 7500000 5
```

The following example shows how to configure spectrum group 3 with an upstream band of 12,000,000 to 18,000,000 Hz and default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 3 band 12000000 18000000
```

The following example shows how to add the upstream band 20,000,000 to 24,000,000 Hz to the list of valid bands with a change in the power level of 13 dBmV for spectrum group 3:

```
Router(config)# cable spectrum-group 3 band 20000000 24000000 13
```

The following example shows how to configure a continuous band between 5,000,004 and 40,000,000 Hz for scheduled spectrum group 4 with a default power level of 0 dBmV. The spectrum group will be available to the spectrum group starting at 12:00 p.m. local time each Monday:

```
Router(config)# cable spectrum-group 4 time Monday 12:00:00 band 5000004 40000000
```

The following example shows how to add the upstream frequency 9,500,000 Hz to the list of valid frequencies and change the nominal power level to 5 dBmV. The spectrum manager adjusts frequencies and power levels on this group at 2:00 a.m. local time each day:

```
Router(config)# cable spectrum-group 3 time 02:00:00 frequency 9500000 5
```

The following example shows how to remove a specified spectrum group from your configuration:

```
Router(config)# no cable spectrum-group 3
Router(config)#
```

Related Commands

Command	Description
cable modulation-profile	Configures preset modulation profiles that you can apply to one or more upstream cable interfaces when you identify and configure spectrum groups.
cable spectrum-group hop period	Sets the minimum frequency-hop interval for a cable spectrum group.
cable spectrum-group hop threshold	Specifies a hop threshold for a cable spectrum group.
cable spectrum-group shared	Specifies the upstream ports in a spectrum group can share the same upstream frequency.
cable upstream frequency	Specifies that the upstream should either be set to a specific center frequency or be set dynamically.
cable upstream power-level	Specifies the upstream cable interface receive power level in dBmV.
cable upstream shutdown	Activates or shuts down a specified upstream cable interface.
cable upstream hopping blind	Disengages the advanced spectrum management features of the Cisco uBR-MC16S and Cisco uBR-MC5X20S cable interface line cards by enabling blind frequency hopping behavior.
show controllers cable	Displays information about the cable interface, including the upstream center frequency.

cable spectrum-group (interface)

To assign a default spectrum group to all of the upstreams on a cable interface, use the **cable spectrum-group** command in interface configuration mode. To remove the spectrum groups from the upstreams, use the **no** form of this command.

cable spectrum-group *group-number*

no cable spectrum-group *group-number*

Syntax Description

group-number Specifies the spectrum group that should be used as the default group for the upstreams on this cable interface. The valid range is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 NA	This command was introduced.
12.2(15)BC2	The maximum number of spectrum groups was increased from 32 to 40 groups per router.

Usage Guidelines

This command assigns a default spectrum group to all of the upstreams on the cable interface. All upstreams on the interface use this spectrum group unless you override this configuration, using one of the following commands:

- To assign a different spectrum group to a particular upstream, use the **cable upstream spectrum-group** command.
- To assign a new frequency to a particular upstream, use the **cable upstream frequency** command.

These two commands override the **cable spectrum-group** command for the particular upstreams to which they are applied. The remaining upstreams in the interface, however, continue to use the default configuration that is specified by the **cable spectrum-group** command.



Tip

You must first create and configure the spectrum groups before you can assign them to an interface. To create and configure spectrum groups, use the set of **cable spectrum-group** commands that are available in global configuration mode.

Examples

The following example shows how to assign spectrum group 1 to all of the upstreams on the cable interface in slot 3/0:

```
Router(config)# interface cable 3/0
```

```
Router(config-if)# cable spectrum-group 1
Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
cable modulation-profile	Configures preset modulation profiles that you can apply to one or more upstream cable interfaces when you identify and configure spectrum groups.
cable spectrum-group (global configuration)	Creates and configures a spectrum group.
cable spectrum-group hop period	Sets the minimum frequency-hop interval for a cable spectrum group.
cable spectrum-group hop threshold	Specifies a hop threshold for a cable spectrum group.
cable spectrum-group shared	Specifies the upstream ports in a spectrum group can share the same upstream frequency.
cable upstream hopping blind	Disengages the advanced spectrum management features of the Cisco uBR-MC16S and Cisco uBR-MC5X20S cable interface line cards by enabling blind frequency hopping behavior.
cable upstream spectrum-group	Assigns a spectrum group to an individual upstream on a cable interface line card.

cable spectrum-group hop period

To change the minimum time between frequency hops, use the **cable spectrum-group hop period** command in global configuration mode. To reset the frequency hop interval for this spectrum group to its default value, use the **no** form of this command.

cable spectrum-group *groupnum* **hop period** *seconds*

no cable spectrum-group *groupnum* **hop period**

Syntax Description

<i>groupnum</i>	Spectrum group number. Valid values are from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.
<i>seconds</i>	Specifies the frequency-hop time period in seconds. Valid values are from 1 to 3600 seconds (before Cisco IOS Release 12.2(8)BC1), or from 1 to 300 seconds (Cisco IOS Release 12.2(8)BC1 or later).

Command Default

Before Cisco IOS Release 12.2(15)BC1: 25 seconds
 Cisco IOS Release 12.2(15)BC1 and later releases: 20 seconds when N+1 HCCP redundancy is not configured, and 15 seconds when N+1 HCCP redundancy is configured on the cable interface

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.1(7)CX1	The default hop period was changed from 300 seconds to 25 seconds to accommodate the new spectrum management features for the Cisco uBR-MC16S spectrum management card.
12.2(8)BC1	The maximum frequency-hop time period was changed from 3600 to 300 seconds.
12.2(15)BC1	The default hop period was changed from 25 seconds to 20 seconds when N+1 HCCP redundancy is not configured on the cable interface, and changed to 15 seconds when N+1 HCCP redundancy is configured.
12.2(15)BC2	The maximum number of spectrum groups was increased from 32 to 40 groups per router.

Usage Guidelines

The **cable spectrum-group hop period** command defines the minimum amount of time that must pass between upstream frequency hops. If ingress noise becomes excessive on a particular upstream, you can set this time period to a smaller value, so as to allow frequency hopping to continue more rapidly until a clear channel is found. Conversely, if the problem appears to be a transient condition, such as a defective CM generating a large volume of errored packets, this time period can be increased to a larger value, so as to avoid excessive frequency hopping by allowing more time between frequency hops.

On the Cisco uBR-MC1xC cards, the maximum recommended hop period is 20 seconds. On the Cisco uBR-MC16S and Cisco uBR-MC5X20S/U cards, the minimum recommended hop period is 25 seconds and the maximum recommended hop period is 35 seconds.

In Cisco IOS Release 12.2(15)BC2, the Cisco CMTS adaptively increases the hop period from the user-defined value to the maximum value (300 seconds) whenever an upstream does not currently have any CMs ranging on it, so as to avoid unnecessary frequency hopping. The user-defined value is restored when a CM starts ranging on the upstream.

**Note**

The hop period should be set to at least 25 seconds on the Cisco uBR-MC16S and Cisco uBR-MC5X20S/U cards so that transient network problems that are unrelated to ingress noise do not generate unnecessary frequency hops.

Examples

The following example shows how to change the minimum frequency-hop interval to 60 seconds. This means that frequency hops for this spectrum group cannot occur more quickly than once every 60 seconds, even if other characteristics, such as exceeding the CNR or FEC threshold values, would normally trigger the hop.

```
Router# configure terminal
Router(config)# cable spectrum-group 1 hop period 60
Router(config)#
```

Related Commands

Command	Description
cable modulation-profile	Creates a cable modulation profile.
cable spectrum-group hop threshold	Specifies a hop threshold for a cable spectrum group.
cable upstream channel-width	Configures an upstream for a range of allowable channel widths.
cable upstream modulation-profile	Configures an upstream for one modulation profile (static profile) or two modulation profiles (Dynamic Upstream Modulation).
show cable hop	Displays the current hop period and threshold for an upstream, along with other statistics.

cable spectrum-group hop threshold

To specify a frequency hop threshold for a spectrum group, use the **cable spectrum-group hop threshold** command in global configuration mode. To delete the hop threshold for this spectrum group, use the **no** form of this command.

cable spectrum-group *groupnum* **hop threshold** [*percent*]

no cable spectrum-group *groupnum* **hop threshold**

Syntax Description

<i>groupnum</i>	Spectrum group number. Valid values are from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.
<i>percent</i>	(Optional) Specifies the frequency hop threshold as a percentage of station maintenance messages that are lost. Valid range is from 1 to 100 percent.

Command Default

20 percent

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.1(7)CX1	The default hop threshold was changed from 100 percent to 20 percent to accommodate the new spectrum management features for the Cisco uBR-MC16S spectrum management card.
12.2(4)BC1	Support for this command was added to the Release 12.2 BC train.
12.2(15)BC2	The maximum number of spectrum groups was increased from 32 to 40 groups per router.

Usage Guidelines

The Cisco CMTS sends a station maintenance message to each CM at least once every 25 to 30 seconds. If a CM does not respond to a station maintenance message within that time period, the CMTS then resends station maintenance messages at a faster rate (typically one second apart) in an attempt to restore connectivity with the CM.

Station maintenance messages can be lost because CMs have lost connectivity with the CMTS, or because ingress noise and other factors are causing dropped and errored packets. Downstream noise can also affect the delivery of station maintenance messages. When a user-configurable percentage of station maintenance messages are lost, the CMTS hops to a new upstream frequency to improve connectivity and sends out an Upstream Channel Descriptor (UCD) update to the CMs to inform them of the change.

The optimal hop threshold value depends on several factors, including the quality of the upstream return path and the number of CMs on the upstream. In addition, the hop threshold works together with the hop period so that transient network problems do not generate an unnecessary number of frequency hops. Ideally, the hop threshold should be set low enough so that the frequency hop can occur before a significant number of CMs go offline, but not so low that it generates frequency hops that are not needed.

For example, if the hop threshold is at its default of 20 percent and an upstream has 100 active CMs, a power outage that affected 20 CMs would usually cause a frequency hop since this is a 20 percent loss of CMs, which in turn would be responsible for at least 20 percent loss of station maintenance messages. But in this situation, the frequency hop would be unneeded because changing the upstream frequency could not correct the original problem (the power outage). If this were a common situation on this upstream, the network administrator might increase the hop threshold so that the repeated power outages would not generate unneeded frequency hops.

If, on the other hand, the power outage affected only 10 CMs, a frequency hop would not occur unless another factor, such as ingress noise, created a sufficient loss of station maintenance messages to reach the 20 percent threshold. In this situation, the default threshold of 20 percent might be sufficient.

Downstream problems can also generate frequency hops. For example, if 20 CMs were on a particularly noisy downstream, over time they could miss a sufficient number of station maintenance messages to generate a frequency hop. The network administrator could increase the hop threshold to limit the possibility of frequency hops due to downstream impairments.

Also, faulty CMs could generate a frequency hop under certain conditions. For example, if a number of faulty CMs generated a large number of uncorrectable forward error correction (FEC) errors or otherwise missed 50 to 60 percent of their station maintenance messages, without actually going offline, over time they could miss a sufficient number of station maintenance messages to cause a frequency hop or modulation change. The network administrator could increase the hop threshold to prevent the CMTS from generating a frequency hop or modulation change for problems such as these, which are unrelated to actual noise on the upstream.

**Note**

If a previous frequency hop had already occurred within the user-configurable hop period, the CMTS will not immediately frequency hop. Instead, the CMTS would wait until the hop period expires, and if the percentage of station maintenance messages still exceeds the hop threshold, the CMTS would perform another frequency hop.

**Tip**

When an upstream has 25 or fewer CMs (which is typical with lab and test environments), the CMTS increases the rate at which it sends station maintenance messages to the CMs. This higher polling rate, along with the small number of CMs, means that frequency hopping can occur more quickly than with a normally loaded upstream, especially when a small number of CMs are powered down or generate noisy traffic.

**Note**

The DOCSIS specification states that when a CM misses 16 sequential station maintenance messages, the CMTS should consider the CM offline and should stop sending station maintenance messages to that CM. The CM must then reregister with the CMTS to resume connectivity.

Examples

The following example shows how to set the threshold that triggers frequency hop to 25 percent of station maintenance messages on the upstream that is assigned to spectrum-group 4:

```
Router# configure terminal
Router(config)# cable spectrum-group 4 hop threshold 25
Router(config)#
```

Related Commands	Command	Description
	cable modulation-profile	Creates a cable modulation profile.
	cable spectrum-group hop period	Sets the minimum frequency-hop interval for a cable spectrum group.
	cable upstream channel-width	Configures an upstream for a range of allowable channel widths.
	cable upstream modulation-profile	Configures an upstream for one modulation profile (static profile) or two modulation profiles (Dynamic Upstream Modulation).
	show cable hop	Displays the current hop period and threshold for an upstream, along with other statistics.

cable spectrum-group shared

To specify that the upstream ports in a spectrum group share the same upstream frequency, use the **cable spectrum-group shared** command in global configuration mode. To delete this specification, use the **no** form of this command.

cable spectrum-group *groupnum* **shared**

no cable spectrum-group *groupnum* **shared**

Syntax Description

groupnum Spectrum group number. Valid values are from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.

Command Default

Upstream port frequency is the same for all ports in the spectrum group.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(11)BC3	Support was added for this command on the Cisco uBR-LCP2-MC16S card on the Cisco uBR10012 router.
12.2(15)BC2	The maximum number of spectrum groups was increased from 32 to 40 groups per router.

Usage Guidelines

Because this command forces upstream ports to use the same spectrum, you must ensure that you do not configure spectrum groups that have overlapping frequencies. To use shared spectrum groups, each group must be using a discrete set of frequencies.



Caution

Depending on the frequencies being used, and how cable modems are distributed across those frequencies and among spectrum groups, switching from a group from shared to non-shared, or from non-shared to shared, could cause CMs in the spectrum group to go offline and begin reranging procedures. You should therefore use this command only during regularly schedule maintenance times, so that a minimum number of online customers are affected.



Note

This command does not enable any sort of load balancing on the shared upstreams.

Examples

The following example shows how to specify that all the upstream ports for spectrum group 4 share the same upstream frequency, and that these upstream frequencies are not assigned to other upstream interfaces:

```
Router(config)# cable spectrum-group 4 shared
Router(config)#
```

Related Commands

Command	Description
cable modulation-profile	Configures preset modulation profiles that you can apply to one or more upstream cable interfaces when you identify and configure spectrum groups.
cable spectrum-group (global configuration)	Creates a spectrum group of one or more frequencies for an upstream.
cable spectrum-group hop period	Sets the minimum frequency-hop interval for a cable spectrum group.
cable spectrum-group hop threshold	Specifies a hop threshold for a cable spectrum group.
cable upstream hopping blind	Disengages the advanced spectrum management features of the Cisco uBR-MC16S and Cisco uBR-MC5X20S cable interface line cards by enabling blind frequency hopping behavior.
show controllers cable	Displays information about the cable interface, including the upstream center frequency.

cable submgmt default

To set the default values for attributes in the Subscriber Management MIB (DOCS-SUBMGT-MIB), and to enable Cisco Static CPE Override on the Cisco CMTS, use the **cable submgmt default** global configuration command. To restore the original defaults, use the **no** form of this command.

```
cable submgmt default [active | learnable | max-cpe cpe-num]
```

```
no cable submgmt default [active | learnable | max-cpe cpe-num]
```

```
cable submgmt default filter-group {cm | cpe | mta | stb | ps} {downstream | upstream} group-id
```

```
no cable submgmt default filter-group {cm | cpe | mta | stb | ps} {downstream | upstream}  
group-id
```

Syntax Description

no	When used with the active and learnable options, the no form of the command sets the default attributes to false. When used with the max-cpe and filter-group options, the no form of the command sets the attribute to 0.
active	(Optional) Sets the docsSubMgtCpeActiveDefault attribute, which controls whether the CMTS manages the CPE devices for a particular CM—when set to TRUE, the CMTS enforces the MAX-CPE value and the implemented filters. The no cable submgmt default active command sets the default value to FALSE (the original default), which turns off CPE management at the CMTS.
learnable	(Optional) Sets the docsSubMgtCpeLearnableDefault attribute, which controls whether the CMTS learns the CPE IP addresses for a particular CM—when set to TRUE (the original default), the CMTS learns IP addresses up to the MAX-CPE value. The no cable submgmt default learnable command sets the default value to FALSE, which means that the IP address for each allowable CPE device must be specified in the DOCSIS configuration file.
max-cpe <i>cpe-num</i>	(Optional) Sets the docsSubMgtCpeMaxIpDefault attribute, which specifies the default number of simultaneous IP addresses (CPE devices) permitted for the CM. The possible range is 0 to 1024, where 0 specifies that all CPE traffic from the CM is dropped. The default is 16.
filter-group	Specifies a filter group, which can be applied to either upstream or downstream traffic for either a CM or its CPE devices.
cm	Specifies that the filter group applies to traffic to or from a CM.
cpe	Specifies that the filter group applies to traffic to or from a CPE device.
mta	Specifies that the filter group applies to traffic to or from a multimedia terminal adaptor (mta.)
stb	Specifies that the filter group applies to traffic to or from a Set-Top Box (stb.)
ps	Specifies that the filter group applies to traffic to or from a portal server (ps.)
downstream	Specifies that the filter group applies to the downstream traffic that is going to the specified CM or CPE device.

upstream	Specifies that the filter group applies to the upstream traffic that is coming from the specified CM or CPE device.
<i>group-id</i>	Specifies the filter group ID (0 to 254) to be applied for the CM or CPE, downstream or upstream filter. This ID references the filter indexes that are used for rows in the docsSubMgtPktFilterTable. A value of 0 indicates that no filtering is used for this particular type of traffic.

Command Default

The Subscriber Management MIB defaults to the following default values:

- The **active** parameter defaults to FALSE (the CMTS does not actively manage CPE devices).
- The **learnable** parameter defaults to TRUE (the CMTS learns the IP addresses for CPE devices).
- The **max-cpe** parameter defaults to 16 IP addresses.
- The filter group ID for each type of filter group defaults to 0, which means that no filtering is done on that type of traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)CX1	This command was introduced.
12.3(9a)BC	This command was integrated into Cisco IOS Release 12.3(9a)BC.
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	This command was updated to support MTA, STB, and portal server.

Usage Guidelines

This command enables field technicians to add a temporary CPE device behind the subscriber's cable modem. The temporary CPE device shares the same SID settings as the original CPE device, even though the temporary CPE device has a different MAC address. The original CPE device automatically changes from *dhcp cpe* to *static cpe* in the CMTS host routing tables, and the CPE device continues to receive service with the same SID.

To disable Cisco CMTS Static CPE Override on the Cisco CMTS, use the **no** form of this command. This automatically updates the routing tables and enables the MAC address from the technician's laptop for a future field service connection at a different location. Prior to using this command, the first (existing) DHCP CPE device maintains its DHCP dynamic MAC address behind the cable modem. The SID is assigned to this IP address.

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

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

**Note**

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

The DOCSIS 1.1 Subscriber Management MIB (DOCS-SUBMGT-MIB) creates and maintains a number of tables that describe the state of subscriber management for the CMs and CPE devices being serviced by the Cisco CMTS. The CMTS creates rows in these tables for each CM and CPE device when the CM registers with the CMTS, and if the CM does not specify a value for an attribute in this table, the CMTS uses the defaults specified by the **cable submgmt default** command.

**Timesaver**

The DOCS-SUBMGT-MIB MIB contains its own default values for these attributes, and those defaults can be overridden by giving the appropriate SNMP SET commands. The **cable submgmt default** command, however, allows the new defaults to be included in the Cisco IOS configuration file so that the defaults are automatically reconfigured whenever the CMTS reboots or reloads.

**Note**

The **cable submgmt default** command sets only the default value for these attributes. These default values are used only if the CM does not specify other values when it registers with the CMTS. If the CM does specify different values at registration time, those values are used instead of these default values.

The attributes in DOCS-SUBMGT-MIB control how the CMTS manages the CPE devices behind a CM and the filters that are applied to the traffic to and from a particular CM and its CPE devices. The following sections describe the relationship between the different forms of the **cable submgmt default** commands and the attributes in DOCS-SUBMGT-MIB.

CPE Management

The first form of the **cable submgmt default** command controls the default values for the entries in the docsSubMgtCpeControlTable, which controls how the CMTS manages the CPE devices for each CM:

cable submgmt default active

Sets the docsSubMgtCpeActiveDefault attribute, which is the default value for the docsSubMgtCpeControlActive attribute in docsSubMgtCpeControlTable. This attribute controls whether the CMTS performs CPE management for a particular CM.

- The **cable submgmt default active** command sets the default to TRUE, which specifies that the CMTS is to manage CPE devices by enforcing the MAX-CPE number and the implemented filters.
- The **no cable submgmt default active** command sets the default to FALSE (the default value), which specifies that the CMTS is not to perform CPE management for the particular CM.

cable submgmt default learnable

Sets the docsSubMgtCpeLearnableDefault attribute, which is the default value for the docsSubMgtCpeControlLearnable attribute in docsSubMgtCpeControlTable. This attribute controls whether the CMTS learns the IP addresses for CPE devices behind a particular CM.

- The **cable submgmt default learnable** command sets the default to TRUE (the default value), which specifies that the CMTS is to learn the IP addresses for the CPE devices behind the CM, up to the value specified by the MAX-CPE parameter. The CMTS learns the IP addresses by monitoring the traffic sent by the CPE devices, and the first CPE devices to transmit traffic are the first CPE devices to be learned.
- The **no cable submgmt default learnable** command sets the default to FALSE, which specifies that the CMTS does not learn the IP addresses for the CPE devices behind a particular CM. Instead, the IP addresses for each CM that is to be allowed access must be specified in the DOCSIS configuration file.

cable submgt default max-cpe *cpe-num*

Sets the docsSubMgtCpeMaxIpDefault attribute, which specifies the default value for the docsSubMgtCpeControlMaxCpeIp attribute in docsSubMgtCpeControlTable. This attribute specifies the maximum number of IP addresses that can transmit traffic through a particular CM. The possible range is 0 to 1024, and the original default is 16.

**Note**

The MAX-CPE attribute is used only when the CMTS is actively managing CPE devices for the CM.

Filter Group Management

The second form of the **cable submgt default** command controls the default values for the entries in the docsSubMgtCmFilterTable, which assigns the CM to one or more filter groups. A filter group specifies what filters are applied to the traffic going to or coming from each particular CM or CPE device. Filter groups can be numbered 0 to 1024, where 0 specifies that no filtering is done for that particular traffic type.

**Note**

The actual filters specified in these commands must be created by setting the appropriate attributes in the DOCS-SUBMGT-MIB MIB using SNMP SET commands.

cable submgt default filter-group cpe downstream *group-id*

Sets the docsSubMgtSubFilterDownDefault attribute, which is the default value for the docsSubMgtSubFilterDownstream attribute in the docsSubMgtCmFilterTable. This attribute applies to downstream traffic that is sent to the CPE devices behind a particular CM.

cable submgt default filter-group cpe upstream *group-id*

Sets the docsSubMgtSubFilterUpDefault attribute, which is the default value for the docsSubMgtSubFilterUpstream attribute in the docsSubMgtCmFilterTable. This attribute applies to upstream traffic that is sent by the CPE devices behind a particular CM.

cable submgt default filter-group cm downstream *group-id*

Sets the docsSubMgtCmFilterDownDefault attribute, which is the default value for the docsSubMgtCmFilterDownstream attribute in the docsSubMgtCmFilterTable. This attribute applies to downstream traffic that is addressed to a particular CM.

cable submgt default filter-group cm upstream *group-id*

Sets the docsSubMgtCmFilterUpDefault attribute, which is the default value for the docsSubMgtCmFilterUpstream attribute in the docsSubMgtCmFilterTable. This attribute applies to upstream traffic that is sent by a particular CM.

**Note**

For more information about using static CPE override, see the Cisco CMTS Static CPE Override feature on Cisco.com.

Examples

The following commands specify that the CMTS defaults to actively managing the CPE devices for each CM that registers, allowing and learning up to four IP addresses for the CPE devices behind that CM.

```
Router# configure terminal
Router(config)# cable submgt default active
Router(config)# cable submgt default learnable
Router(config)# cable submgt default max-cpe 4
```

The following commands specify that the CMTS defaults to actively managing the CPE devices for each CM that registers. Each CM, however, must specify its own MAX-CPE value; otherwise, that value defaults to 0 and all traffic to and from the CPE devices for that CM is blocked.

```
Router# configure terminal
Router(config)# cable submgmt default active
Router(config)# cable submgmt default max-cpe 0
```

The following commands specify that the CMTS defaults to not actively managing the CPE devices for each CM that registers. However, if the CM at registration time indicates that the CMTS is to actively manage the CPE devices, the CMTS defaults to allowing only one CPE device. Learning also is disabled, so that one CPE device, therefore, must be specified in the DOCSIS configuration file that the CM uses to register.

```
Router# configure terminal
Router(config)# no cable submgmt default active
Router(config)# no cable submgmt default learnable
Router(config)# cable submgmt default max-cpe 1
```

The following commands specify that the CMTS defaults to assigning three filter groups to each CM that registers. Unless the CM indicates otherwise at registration time, downstream and upstream traffic for the CPE devices behind the CM is filtered according to the rules for filter groups 20 and 21, respectively. Filter group 1 is applied to the downstream traffic addressed to the CM. Upstream traffic sent by the CM, however, is not filtered.

```
Router# configure terminal
Router(config)# cable submgmt default filter-group cpe downstream 20
Router(config)# cable submgmt default filter-group cpe upstream 21
Router(config)# cable submgmt default filter-group cm downstream 1
Router(config)# cable submgmt default filter-group cm upstream 0
```

**Note**

The above example assumes that filter groups 1, 20, and 21 have already been created on the CMTS using the appropriate SNMP commands.

Related Commands

Command	Description
cable filter group	Creates a DOCSIS 1.1 filter group that filters packets on the basis of the TCP/IP and UDP/IP headers.

cable sync-interval

To specify the interval between successive sync message transmissions from the Cisco CMTS, use the **cable sync-interval** command in cable interface configuration mode. To return the sync message interval to its default value, use the **no** form of this command.

cable sync-interval *msec*

no cable sync-interval

Syntax Description	<i>msec</i> Specifies the interval in milliseconds (ms) between successive sync message transmissions from the Cisco CMTS. Valid values are from 1 to 200 ms. Default value is 10 ms.	
Command Default	10 ms	
Command Modes	Interface configuration (cable interface only)	
Command History	Release	Modification
	11.3 NA	This command was introduced.
Usage Guidelines	To verify whether or not a sync message interval has been configured, enter the show running-config command and look for the cable interface configuration information. If a sync message interval has been configured, it appears in this output. If the sync message interval has been deactivated or reset to its default value, no sync interval command line appears in the output.	
Examples	The following example shows how to specify the interval for the sync message transmissions to 100 ms: Router (config-if)# cable sync-interval 100	