Cable Commands: q through sg

Revised: July 2012, OL-15510-15

New Commands

Command	Cisco IOS Software Release
rf-channel network-delay	12.3(23)BC
session-range	12.2(33)SCA
rcp id	12.2(33)SCB
receive channel	12.2(33)SCB
receive module	12.2(33)SCB
revertive	12.2(33)SCA
service divert-rate-limit ip	12.2(33)SCB
service divert-rate-limit ip trusted-site	12.2(33)SCB
service divert-rate-limit non-ip	12.2(33)SCB
service divert-rate-limit trusted-site	12.2(33)SCB
restricted	12.2(33)SCC
rf-channel depi-tunnel	12.2(33)SCC
rf-channel rf-power	12.2(33)SCC
rf-channel rf-shutdown	12.2(33)SCC
service class(cmts-tag)	12.2(33)SCC
service-type-id	12.2(33)SCC
service-type-id(cmts-tag)	12.2(33)SCC
service instance	12.2(33)SCC
rf-channel stacking	12.2(33)SCD
rf-switch auxport enable	12.2(33)SCG

Modified Commands

Command	Cisco IOS Software Release
redundancy force-switchover	12.2(33)SCA
service class	12.2(33)SCA
rf-channel frequency	12.3(23)BC
rf-channel ip-address mac-address udp-port	12.3(23)BC
rf-channel frequency	12.2(33)SCB
rf-channel ip-address mac-address udp-port	12.2(33)SCB
rf-channel network-delay	12.2(33)SCB
rf-channel network-delay	12.2(33)SCC
rf-channel rf-power	12.2(33)SCD
service divert-rate-limit ipv6	12.2(33)SCE
s**ervice divert-rate-limit trusted-site-ipv6**	12.2(33)SCE

Removed Commands

Command	Cisco IOS Software Release
service divert-rate-limit	12.2(33)SCB
redundancy linecard-group	12.2(33)SCE

qos-profile enforced

To specify a quality-of-service (QoS) profile that should be enforced when users violate their registered QoS profiles, use the **qos-profile enforced** command in enforce-rule configuration mode. To delete the enforced QoS profile from the enforce-rule, use the **no** form of this command.

> **qos-profile enforced** *profile-id* [**no-persistence**]

> **no qos-profile enforced** *profile-id* [**no-persistence**]

Syntax Description		
	profile-id	Specifies the QoS profile to be enforced. The valid range is 0 to 16383, with a default of 0.
	no-persistence	(Optional) Specifies that the enforced QoS profile should not remain in force when a cable modem reboots. Instead, when a cable modem that is in the penalty period reboots, it is automatically removed from the penalty period and assigned the QoS profile that is specified in its DOCSIS configuration file.
		The default behavior is that enforced QoS profiles remain in force for cable modems across reboots.

Command Default The value of *profile-id* defaults to 0, and enforced QoS profiles are persistent across cable modem reboots.

Command Modes Enforce-rule configuration (enforce-rule)

Command History	Release	Modification
	12.3(9a)BC	This command was introduced. This command replaces the **enforced qos-profile** command.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines Both the originally provisioned QoS profile and the enforced QoS profile must be created on the Cisco CMTS router. The *profile-id* does not support QoS profiles that are created by the cable modem.

An enforce-rule can specify an enforced QoS profile, which is automatically applied to subscribers who transmit more traffic than allowed by their registered QoS profile. The enforced QoS profile remains in effect during the penalty time period (see the **penalty-period** command). At the end of the penalty period, the subscriber returns to the registered QoS profile.

If a cable modem reboots while it is in its penalty time period, it continues using the enforced QoS profile, unless the service provider has manually changed the cable modem's registered QoS profile using the **cable modem qos profile** command.

When you change the enforced QoS profile for a currently active enforce-rule, any cable modems using this rule that are currently in the penalty period continue using the previously configured enforced QoS profile. Any cable modems that enter the penalty period after this configuration change, however, use the new enforced QoS profile.

An enforced QoS profile must already have been created on the Cisco CMTS router before you can assign it to an enforce-rule. If the rule does not exist, the system displays an error message.

When the **no-persistence** option is specified, the enforced QoS profile is still automatically applied to subscribers who violate their bandwidth requirements. However, when the cable modem reboots, the Cisco CMTS router allows the cable modem to use the QoS profile that is specified in its DOCSIS configuration file.

The **no-persistence** option can be used when initially using the Subscriber Traffic Management feature to identify potential problem applications and users. When repeat offenders are identified, they can then be assigned enforce-rules that do not use the **no-persistence** option, so that they remain in the penalty period even if they reboot their cable modems.

> **Note**   The system automatically applies the enforced QoS profile to violators only if the **enforce** keyword has been used with the **activate-rule-at-byte-count** command.

Examples   The following example shows profile 12 being assigned as the enforced QoS profile to an enforce-rule:

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# qos-profile enforced 12
```

The following example shows profile 12 being assigned as the enforced QoS profile to an enforce-rule, but with the **no-persistence** option specified, so that the enforced QoS profile does not remain in force if the cable modem reboots:

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# qos-profile enforced 12 no-persistence
```

The following example shows the error message that is displayed when the specified QoS profile does not exist on the CMTS:

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# qos-profile enforced 98

The qos profile 98 doesn't exist or it's a cm created QoS profile
```

Related Commands

Command	Description
cable qos enforce-rule	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
debug cable subscriber-monitoring	Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.
duration	Specifies the time period and sample rate to be used for monitoring subscribers.

Command	Description
enabled (enforce-rule)	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.
monitoring-basics	Specifies the type of monitoring for subscriber traffic management on a Cisco CMTS router.
peak-time1	Specifies peak and offpeak monitoring times on a Cisco CMTS router.
qos-profile registered	Specifies the registered QoS profile that should be used for this enforce-rule.
service-class (enforce-rule)	Identifies a particular service class for cable modem monitoring in an enforce-rule.
show cable qos enforce-rule	Displays the QoS enforce-rules that are currently defined.
show cable subscriber-usage	Displays subscribers who are violating their registered QoS profiles.

qos-profile registered

To specify the registered quality of service (QoS) profile that should be used for this enforce-rule, use the **qos-profile registered** command in enforce-rule configuration mode. To remove the registered QoS profile from the enforce-rule, use the **no** form of this command.

qos-profile registered *profile-id*

no qos-profile registered *profile-id*

Syntax Description

profile-id	Specifies the QoS profile to be monitored. This profile must be created on the Cisco CMTS router. If you want to manage a cable modem that uses a modem-created QoS profile, you must first create that exact QoS profile on the CMTS router before using this command. The valid range is 0 to 16383, with a default of 0.

Command Default   The default profile ID is 0.

Command Modes   Enforce-rule configuration (enforce-rule)

Command History

Release	Modification
12.3(9a)BC	This command was introduced. This command replaces the **registered qos-profile** command.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines   You must specify a registered QoS profile for each enforce-rule. The Cisco CMTS router then uses the registered profile ID to match subscribers' service flows to the proper enforce-rules.

When you change the registered QoS profile for an active rule, the cable modems that had been using the previous registered QoS profile are no longer managed by the Cable ARP Filtering feature. Instead, the rule begins managing those cable modems that use the new registered QoS profile.

Note   The registered QoS profile must be created on the Cisco CMTS router before you can assign it to an enforce-rule. If the rule does not exist, the system displays an error message. If you want to manage a cable modem that is currently using a modem-created QoS profile, you must first manually create a new QoS profile on the CMTS router that has the same QoS parameters as the modem-created profile. Then allow the modem to come online using the manually created profile, before using the **qos-profile registered** command.

Examples The following example shows profile 50 being assigned as the registered QoS profile to an enforce-rule:

```
Router# configure terminal
Router(config)# cable qos enforce-rule enforce-rule
Router(enforce-rule)# qos-profile registered 50
```

The following example shows the error message that is displayed when the specified QoS profile does not exist on the CMTS:

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# qos-profile registered 99

The qos profile 99 doesn't exist or it's a cm created QoS profile
```

Related Commands

Command	Description
cable qos enforce-rule	Creates an enforce-rule to to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
debug cable subscriber-monitoring	Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.
duration	Specifies the time period and sample rate to be used for monitoring subscribers.
enabled (enforce-rule)	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.
monitoring-basics	Specifies the type of monitoring for subscriber traffic management on a Cisco CMTS router.
peak-time1	Specifies peak and offpeak monitoring times on a Cisco CMTS router.
qos-profile enforced	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles.
service-class (enforce-rule)	Enables the enforcing of QOS profiles according to service class.
show cable qos enforce-rule	Displays the QoS enforce-rules that are currently defined.
show cable subscriber-usage	Displays subscribers who are violating their registered QoS profiles.

rcp-id

To assign a receive channel profile (RCP) ID to a receive channel configuration (RCC) template, use the **rcp-id** command in RCC template configuration mode. To remove the RCP ID, use the **no** form of this command.

rcp-id *rcp-id*

no rcp-id *rcp-id*

Syntax Description	*rcp-id*	Specifies an RCP ID for the RCC template. The valid range is from 00 00 00 00 00 to FF FF FF FF FF.

Command Default   By default the RCP ID is set to 00 00 00 00 00. However, you must change the default value to a non-zero RCP ID.

Command Modes   RCC template configuration (config-rcc-template)

Command History

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

Usage Guidelines   A valid RCC template consists of a configured RCP ID, a receive module (RM) entry, and a receive channel (RC) entry.

First, you define an RCC template for an RCP, and then assign the template to a cable interface to generate RCCs based on the actual DS channel configuration.

Examples   The following example shows how to assign an RCP ID to an RCC template:

```
Router# configure terminal
Router(config)# cable rcc-template 1
Router(config-rcc-template)# rcp-id 00 10 00 00 03
```

Related Commands

Command	Description
rcp-id	Specifies an ID for the receive channel profile.
receive-module	Specifies a receive module entry in the form of a numeric value.
receive-channel	Specifies a receive channel entry in the form of a numeric value.

receive-channel

To associate a receive channel to a receive module (RC), use the **receive-channel** command in RCC template configuration mode. To restore the default value, use the **no** form of this command.

receive-channel *index* **center-frequency** *Hz* **connected-receive-module** *index* [**primary**]

no receive-channel *index* **center-frequency** *Hz* **connected-receive-module** *index*

Syntax Description

index	Specifies the index value for the receive channel. The valid range is 1 to 10.
center-frequency	Specifies the center frequency for the receive channel.
Hz	Specifies the center frequency value in Hz. The valid range is 55000000-858000000.
connected-receive-module	Specifies a nested receive module in the RCC template. Generally, only one receive module is configured for an RCC template.
index	Specifies the index value for the connected receive module. The valid range is 1 to 10.
Primary	(Optional) Indicates that it is a CM primary channel and an RCC can be derived from this channel.

Command Default   .No default behavior or values.

Command Modes   RCC template configuration (config-rcc-template)

Command History

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

Usage Guidelines   A valid RCC template consists of a configured RCP ID, a receive module (RM) entry, and a receive channel (RC) entry. First, you define an RCC template for an RCP, and then assign the template to a cable interface to generate RCCs based on the actual DS channel configuration.

An RCC template configures the physical layer components described by an RCP, including receive modules and receive channels to specific downstream frequencies, and specifies the interconnections among receive modules or between receive modules and receive channels.

A receive module can include multiple receive channels. So we need to specify which receive channel belongs to which receive module.

Examples   The following example shows how to associate a receive channel to a receive module:

```
Router# configure terminal
Router(config)# cable rcc-template 1
Router(config-rcc-template)# rcp-id 00 10 00 00 03
Router(config-rcc-template)# receive-module 1 first-channel-center-frequency 555000000
Router(config-rcc-template)# receive-channel 1 center-frequency 555000000
connected-receive-module 1 primary
Router(config-rcc-template)# receive-channel 2 center-frequency 561000000
connected-receive-module 1
```

Related Commands

Command	Description
cable rcc-template	Defines a receive channel configuration (RCC) template for an RCP.
rcp-id	Specifies an ID for the receive channel profile.
receive-module	Specifies a receive module entry in the form of a numeric value.

receive-module

To associate a receive module (RC) to a Receive Channel Configuration (RCC) template, use the **receive-module** command in RCC template configuration mode. To restore the default value, use the **no** form of this command.

> **receive-module** *index* **first-channel-center-frequency** *Hz* [**connected-receive-module** *index*]

> **no receive-module** *index* **first-channel-center-frequency** *Hz* [**connected-receive-module** *index*]

Syntax Description

index	Specifies the index value for the receive module. The valid index range is 1 to 10.
first-channel-center-frequency	Specifies the center frequency of the first channel of the receive module channel block.
Hz	Specifies the center frequency value in Hz. The valid range is 55000000 to 858000000.
connected-receive-module	(Optional) Specifies a nested receive module in the RCC template. Generally, only one receive module is configured for an RCC template.
index	(Optional) Specifies the index value for the connected receive module. The valid range is 1 to 10.

Command Default

.No default behavior or values.

Command Modes

RCC template configuration (config-rcc-template)

Command History

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

Usage Guidelines

A valid RCC template consists of a configured RCP ID, a receive module (RM) entry, and a receive channel (RC) entry. First, you define an RCC template for an RCP, and then assign the template to a cable interface to generate RCCs based on the actual DS channel configuration.

An RCC template configures the physical layer components described by an RCP, including receive modules and receive channels to specific downstream frequencies, and specifies the interconnections among receive modules or between receive modules and receive channels.

A receive module can include multiple receive channels. So we need to specify which receive channel belongs to which receive module.

Examples   The following example shows how to associate a receive module to an RCC template:

```
Router# configure terminal
Router(config)# cable rcc-template 1
Router(config-rcc-template)# rcp-id 00 10 00 00 03
Router(config-rcc-template)# receive-module 1 first-channel-center-frequency 555000000
Router(config-rcc-template)# receive-channel 1 center-frequency 555000000
connected-receive-module 1 primary
Router(config-rcc-template)# receive-channel 2 center-frequency 561000000
connected-receive-module 1
```

Related Commands

Command	Description
cable rcc-template	Defines a receive channel configuration (RCC) template for an RCP.
rcp-id	Specifies an ID for the receive channel profile.
receive-channel	Specifies a receive channel entry in the form of a numeric value.

redundancy force-failover main-cpu

To force a switchover, so that the standby Performance Routing Engine (PRE1) module becomes the active PRE1 module, use the **redundancy force-failover main-cpu** command in privileged EXEC mode.

redundancy force-failover main-cpu

Syntax Description   This command has no keywords or arguments.

Defaults   No default behavior or values

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
12.2(4)XF1	This command was introduced for the Cisco uBR10012 router.
12.2(11)BC3	The active PRE1 module checks to see if a switchover is currently in progress before implementing this command.
12.3(21)BC	This command is replaced by the **redundancy switch-activity** command.

Usage Guidelines   The **redundancy force-failover main-cpu** command initiates a manual switchover, so that the standby PRE1 module becomes the active PRE1 module and assumes full responsibilities for router operations. This command requires that both PRE1 modules are running a Cisco IOS software image that supports the Route Processor Redundancy (RPR) feature.

Note   The terms failover and switchover are interchangeable, but switchover is the term used across all Cisco platforms capable of high-availability operation.

A manual switchover is typically done for one of the following reasons:

- You want to upgrade or replace the active PRE1 module.

- You have upgraded the Cisco IOS software on the standby PRE1 module and want the standby PRE1 module to begin using the new software image. This also allows you to upgrade the software on the former active PRE1 module without interrupting systems operations.

- You want to test switchover operation on the system.

A switchover can also be manually initiated by removing the active PRE1 module from the chassis, but using the **redundancy force-failover main-cpu** command provides a more graceful switchover, without generating hardware alarms.

Tip Do not perform a switchover immediately after you change the configuration and save it to the NVRAM. Instead, wait a few minutes to allow the two PRE1 modules to synchronize the new configuration, and then perform the switchover.

Tip Wait two to three minutes after a switchover before switching the system back to the original PRE1 module, so as to allow the system to stabilize and so that both PRE1 modules are ready for the switch. In Cisco IOS Release 12.2(11)BC3 and later releases, the active PRE1 module will not initiate a new switchover until a current switchover is complete and the system has stabilized.

Examples   The following example shows a switchover being manually initiated:

```
Router# redundancy force-failover main-cpu
Proceed with switchover to standby PRE? [confirm] y
```

Note Pressing **enter** or **y** confirms the action and begins the switchover. Pressing any other key aborts the switchover and returns control to the current active PRE1 module.

The following example shows a switchover being attempted but failing because the standby PRE1 module is either not ready, not available, or not installed:

```
Router# redundancy force-failover main-cpu

Proceed with switchover to standby PRE? [confirm]
Standby PRE not ready, switchover aborted.
Router#
```

Note In some versions of Cisco IOS software, a failed software switchover will show the following message:

```
Unable to communicate with standby PRE, switchover aborted.
```

Related Commands

Command	Description
associate	Associates two line cards for Automatic Protection Switching (APS) redundancy protection.
redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
redundancy reload	Resets the standby PRE1 module or to reset both the active and standby PRE1 modules.
redundancy switch-activity	Forces a switchover to the standby PRE module.

redundancy force-switchover main-cpu

To force a standby Performance Routing Engine (PRE) to assume the role of an active PRE, use the **redundancy force-switchover main-cpu** command in privileged EXEC mode.

> **redundancy force-switchover main-cpu**

Syntax Description   None.

Command Default   This command has no default behavior or values.

Command Modes   Privileged EXEC (#)

Command History

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

Usage Guidelines   Before using this command, install the Cisco IOS software image (to ensure high availability), and configure the Route Processor Redundancy (RPR) mode on both the PRE modules.

> **Note**   The terms failover and switchover are interchangeable, but switchover is the term used across all Cisco platforms capable of high-availability operation.

> **Note**   We recommend you use the **redundancy force-switchover main-cpu** command only on the active PRE module. The active PRE crashes used on the standby PRE.

Examples   The following example shows a manual switchover:

```
Router# redundancy force-switchover main-cpu
Proceed with switchover to standby PRE? [confirm] y
Preparing to Switch Activity
```

> **Note**   Pressing **enter** or **y** confirms the action and begins the switchover. Pressing any other key aborts the switchover and returns control to the currently active PRE module.

The following example shows a switchover being attempted but failing because the standby PRE module is either not ready, not available, or not installed:

```
Router# redundancy force-switchover main-cpu

Proceed with switchover to standby PRE? [confirm] n

Standby PRE not ready, switchover aborted.
```

Cisco IOS CMTS Cable Command Reference ■

```
Router#
```

	Command	Description
Related Commands	**redundancy**	Enters the redundancy configuration mode so that the synchronization parameters could be configured.
	redundancy reload	Resets the standby PRE module or resets both the active and standby PRE modules.
	redundancy switch-activity	Forces a switchover to the standby PRE module.
	show redundancy	Displays the current active and standby Supervisor card redundancy status.

redundancy reload

To manually reload a standby Route Processor (RP) module, use the **redundancy reload** command in privileged EXEC mode.

> **redundancy reload** {**peer** | **shelf**}

Syntax Description

peer	Reloads only the standby PRE1 module or Supervisor card.
shelf	Reloads both the active and standby PRE1 module or Supervisor card.

Defaults   No default behavior or values

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
12.2(4)XF1	This command was introduced for the Cisco uBR10012 router.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was removed from Cisco IOS Release 12.2(33)SCA. It is replaced by the **hw-module standby-cpu reset** command.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.
15.2(4)M	This command was introduced.

Usage Guidelines   The **redundancy reload peer** command is used to reset the standby RP module when there are any failures, tracebacks, or functionality and behavior mismatches on either one or both active and standby RP modules.

This command does not have an impact on active device operations, assuming a switchover is not required while the standby module is resetting.

The **redundancy reload shelf** command reloads the Cisco IOS software on both the active and standby RP modules. This command interrupts services on the router until all the RP modules and the line cards initialize and come back online.

Examples   The following example shows how to manually reload the standby RP module:

```
Router# redundancy reload peer
Reload peer? [confirm] y
Preparing to reload peer
```

Note   Pressing **enter** or **y** begins the reload. Pressing any other key aborts the reload and returns control to the active RP module.

The following is sample output when a standby RP module is not installed on a router:

```
Router# redundancy reload peer
System is running in SIMPLEX mode, reload anyway? [confirm] n
Peer reload not performed.
```

The following example shows how to reload all RP modules:

```
Router# redundancy reload shelf

Reload the entire shelf [confirm] y
Preparing to reload entire shelf
```

Note Pressing **enter** or **y** begins the reload. Pressing any other key aborts the reload and returns control to the current active PRE1 module.

Cisco RF Gateway 10

The following example shows the system response when a standby Supervisor card is not installed in the Cisco RFGW-10:

```
Switch# redundancy reload peer

System is running in SIMPLEX mode, reload anyway? [confirm] n
Peer reload not performed.
```

The following example shows how to reload both Supervisor cards on the Cisco RFGW-10:

```
Switch# redundancy reload shelf

Reload the entire shelf [confirm] y
Preparing to reload entire shelf
```

Note Pressing **Enter** or **y** confirms the action and begins the reload of both cards. Pressing any other key aborts the reload and returns control to the current active Supervisor card.

Related Commands	Command	Description
	associate slot	Associates slots for APS processor redundancy.
	redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
	redundancy force-failover main-cpu	Forces a switchover, so that the standby RP module becomes the active RP module.
	redundancy switch-activity	Forces a switchover to the standby RP module.

redundancy switch-activity

To force a switchover to the standby PRE module, use the **redundancy switch-activity** command in privileged EXEC mode.

redundancy switch-activity [**force**]

✎
Note   The terms failover and switchover are interchangeable, but switchover is the term used across all Cisco platforms capable of high-availability operation.

Syntax Description

force	(Optional) Forces a switchover immediately, overriding any checks in the code or configuration that might prevent or delay a switchover.

Command Default   No default behavior or values

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(4)XF1	This command was introduced for the Cisco uBR10012 router.

Usage Guidelines   The **redundancy switch-activity** command is similar to the **redundancy force-failover main-cpu** command, except that it includes an option to force the switchover, overriding any configuration checks or other checks in the software that could prevent the switchover. In all cases, this command verifies that the standby PRE module is available and capable of performing the switchover before it transfers control to that PRE module. This command also synchronizes the current running-config and client data before initiating the switchover.

Examples   The following example shows a switchover being manually initiated, overriding any checks that might prevent or delay the switchover:

```
Router# redundancy switch-activity force
Proceed with switchover to standby PRE? [confirm] y
```

✎
Note   Pressing **enter** or **y** confirms the action and begins the switchover. Pressing any other key aborts the switchover and returns control to the current active PRE1 module.

Related Commands

Command	Description
associate	Associates two line cards for Automatic Protection Switching (APS) redundancy protection.
redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
redundancy reload	Resets the standby PRE1 module or to reset both the active and standby PRE1 modules.
redundancy force-failover main-cpu	Forces a switchover, so that the standby Performance Routing Engine (PRE1) module becomes the active PRE1 module.

registered qos-profile

✎

Note   Effective with Cisco IOS Release 12.3(9a)BC, the **registered qos-profile** command is replaced by the **qos-profile registered** command.

To specify the registered quality of service (QoS) profile that should be used for this enforce-rule, use the **registered qos-profile** command in enforce-rule configuration mode. To remove the registered QoS profile from the enforce-rule, use the **no** form of this command.

registered qos-profile *profile-id*

no registered qos-profile *profile-id*

Syntax Description

profile-id	Specifies the QoS profile to be monitored. This profile must be created on the Cisco CMTS router. If you want to manage a cable modem that uses a modem-created QoS profile, you must first create that exact QoS profile on the CMTS router before using this command. The valid range is 0 to 16383, with a default of 0.

Command Default   The default profile ID is 0.

Command Modes   Enforce-rule configuration (enforce-rule)

Command History

Release	Modification
12.2(15)BC1	This command was introduced.
12.3(9a)BC	This command was replaced by the **qos-profile registered** command.

Usage Guidelines   You must specify a registered QoS profile for each enforce-rule. The Cisco CMTS router then uses the registered profile ID to match subscribers' service flows to the proper enforce-rules.

When you change the registered QoS profile for an active rule, the cable modems that had been using the previous registered QoS profile are no longer managed by the Subscriber Traffic Management feature. Instead, the rule begins managing those cable modems that use the new registered QoS profile.

✎

Note   The registered QoS profile must be created on the Cisco CMTS router before you can assign it to an enforce-rule. If the rule does not exist, the system displays an error message. If you want to manage a CM that is using a CM-created QoS profile, you must first create a QoS profile on the Cisco CMTS router that matches the CM-created profile exactly. Then use the **registered qos-profile** command to assign that profile to this enforce-rule.

Examples The following example shows profile 50 being assigned as the registered QoS profile to an enforce-rule:

```
Router# configure terminal
Router(config)# cable qos enforce-rule enforce-rule
Router(enforce-rule)# registered qos-profile 50
```

The following example shows the error message that is displayed when the specified QoS profile does not exist on the CMTS:

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# registered qos-profile 99

The qos profile 99 doesn't exist or it's a cm created QoS profile
```

Related Commands

Command	Description
activate-rule at-byte-count	Specifies the number of bytes that a subscriber can transmit during the monitoring period on a Cisco CMTS router.
cable qos enforce-rule	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
duration	Specifies the time period and sample rate to be used for monitoring subscribers.
enabled (enforce-rule)	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.
penalty-period	Specifies the time period that an enforced QoS profile should be in effect for subscribers that violate their registered QoS profiles.
qos-profile enforced	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles.
show cable qos enforce-rule	Displays the QoS enforce-rules that are currently defined.
show cable subscriber-usage	Displays subscribers who are violating their registered QoS profiles.

restricted

To convert a general load balancing group (GLBG) to a restricted load balancing group (RLBG) for DOCSIS load balancing, use the **restricted** command in the config-lb-group configuration mode. To revert to the general group type for DOCSIS load balancing, use the **no** form of this command.

restricted

no restricted

Command Default By default, the general group type is selected for load balancing.

Command Modes DOCSIS load balancing group mode (config-lb-group)

Command History

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

Examples The following example shows how to convert a GLBG to a RLBG using the **restricted** command.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# restricted
Router(config-lb-group)#
```

Related Commands

Command	Description
cable load-balance docsis-group	Configures a DOCSIS load balancing group on the CMTS.
show cable load-balance docsis-group	Displays real-time configuration, statistical, and operational information for load balancing operations on the router.

revertive

To enable the revert operation on a protect card, use the **revertive** command in line card redundancy group mode.

revertive *time*

no revertive *time*

Syntax Description	*time* Specifies the revert operation time in minutes. The valid values are 1 to 35791.

Command Default   None

Command Modes   Line card redundancy group (config-red-lc)

Command History

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

Examples   The following example shows how to specify the revert operation time for a protect card on a uBR10012 router:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# revertive 30
```

Related Commands

Command	Description
linecard-group	Creates a line card group for one-to-one line card redundancy.
redundancy	Enters redundancy mode.
member subslot	Enables the redundancy role of a line card.

rf-channel cable downstream channel-id

To assign a downstream channel ID to an RF channel, use the **rf-channel cable downstream channel-id** command in controller configuration mode. To remove a downstream channel ID for an RF channel, use the **no** form of this command.

rf-channel *rf-port* **cable downstream channel-id** *channel-id*

no rf-channel *rf-port* **cable downstream channel-id** *channel-id*

Syntax Description

rf-port	Specifies the RF channel physical port on the Wideband SPA FPGA. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command.
channel-id	A unique channel ID. Valid values for releases prior to Cisco IOS Release 12.2(33)SCB are from 0 to 255 and the valid values for Cisco IOS Release 12.2(33)SCB and later are from 1 to 255 as 0 is reserved for network management.

Command Default   If the **rf-channel cable downstream channel-id** command is not issued, Cisco IOS software assigns a unique downstream channel ID to the RF channel.

Command Modes   Controller configuration (config-controller)

Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCB1	The downstream channel ID scheme was changed.

Usage Guidelines   For the wideband channel to work correctly, each RF channel on the fiber node that the wideband channel uses must have a unique downstream channel ID. By default, Cisco IOS software assigns a unique downstream channel ID to the RF channel. Use the **rf-channel cable downstream channel-id** command to change the default channel ID.

The downstream channel ID that is assigned to the RF channel must be unique on the fiber node.

- The ID cannot be the same ID as is used for another RF channel on the fiber node.
- The ID cannot be the same ID as is used for a primary downstream channel on the fiber node.

You can check downstream channel IDs that are being used by examining the CMTS router configuration file.

Refer to **cable downstream channel-id** *id* command for the updated downstream channel ID scheme table.

> **Note**
> If you assign a downstream channel ID that is not unique on the fiber node, the **rf-channel cable downstream channel-id** command displays an error message. The command does assign the channel ID, but the status of the fiber node becomes invalid.

The Cisco uBR10012 router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels depending on how the SPA is configured with the **annex modulation** command.

- For annex A and 256 QAM, each Wideband SPA supports 18 RF channels. In this case, valid values for the *rf-port* argument are 0 to 17.

- For all other cases, the SPA supports 24 RF channels. In these cases, valid values for the *rf-port* argument are 0 to 23.

> **Note**
> Effective with Cisco IOS Release 12.3(23)BC, the **annex modulation** command is obsolete and **annex** and **modulation** are included as keyword options in the **rf-channel frequency** command. Also, for annex A and 256 QAM, each Wideband SPA supports up to 18 RF channels at full rate or up to 24 RF channels at less than full rate.

Examples
The following example shows how to assign a downstream channel ID of 123 to RF channel 3 on the Wideband SPA located in slot/subslot/bay 1/0/1.

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/1
Router(config-controller)# rf-channel 3 cable downstream channel-id 123
```

Related Commands

Command	Description
annex modulation	Sets the annex and modulation for the Wideband SPA.
cable primary	Specifies that a wideband channel is a primary wideband channel.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel.
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
ip-address (controller)	Sets the IP address of the Wideband SPA FPGA.
modular-host subslot	Specifies the modular-host line card.
rf-channel frequency	Sets the frequency for each RF channel.
rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address and UDP port for each RF channel.
rf-channel network delay	Specifies the CIN delay for each RF channel.
rf-channel description	Specifies the description for each RF channel.

rf-channel depi-tunnel

To bind the depi-tunnel, which inherits the configuration of the specified l2tp-class and depi-class, to an rf-channel on a shared port adapter (SPA), use the **rf-channel depi-tunnel** command in controller configuration mode. The **tsid** keyword is used to associate the logical rf-channel of the SPA to a physical quadrature amplitude modulation (QAM) on the radio frequency gateway (RFGW-10). To unbind the depi-tunnel, use the **no** form of this command.

> **rf-channel** *rf-channel* **depi-tunnel** *depi-tunnel-name* **tsid** *id*

> **no rf-channel** *rf-channel* **depi-tunnel** *depi-tunnel-name* [**tsid** *id*]

Syntax Description

rf-channel	RF channel physical port on the Wideband SPA. The allowed range is from 0 to 3.
depi-tunnel-name	Name of the DEPI tunnel.
tsid *id*	TS ID value.

Command Default   This command has no default behavior or values.

Command Modes   Global configuration (config)

Subinterface configuration (config-subif)

Command History

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

Usage Guidelines   To configure DEPI on the M-CMTS, bind the depi-tunnel to an rf-channel on a SPA using the **rf-channel depi-tunnel** command in controller configuration mode. To associate the logical rf-channel on the SPA to a QAM on the RFGW, use the **tsid** keyword.

Examples   The following example shows how to bind the depi-tunnel SPA0 to rf-channel 0 on a SPA and associate tsid 100 to the QAM:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 depi-tunnel SPA0 tsid 100
```

Related Commands	**Command**	**Description**
	controller modular-cable	Specifies the slot, bay, and port to be configured.
	show interface modular-cable	Displays the DEPI information for the modular cable.

rf-channel description

To configure the description of an RF channel on a Wideband SPA, use the **rf-channel description** command in controller configuration mode. To remove an RF channel configuration, use the **no** form of this command.

> **rf-channel** *rf-port* **description** *description*

> **no rf-channel** *rf-port* **description** *description*

Syntax Description		
rf-port	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command (see the Usage Guidelines section).
description	Specifies a description for the RF channel.

Command Default   No default RF channel configuration values are set for the description.

Command Modes   Controller configuration (config-controller)

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

Usage Guidelines   The Cisco uBR10012 router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels depending on how the SPA is configured with the **annex modulation** command. For annex A and 256 QAM, each Wideband SPA supports up to 18 RF channels at full rate and up to 24 RF channels at less than full rate. For all other cases, the SPA supports 24 RF channels.

Note   In Cisco IOS Release 12.3(21)BC, annex and modulation parameters were set globally for each SPA using the **annex modulation** command.
Beginning in Cisco IOS Release 12.3(23)BC, annex and modulation values are set for each RF channel using the **rf-channel frequency** command. The **annex modulation** command is obsolete.

Examples   The following example shows how to configure the description of the RF channel characteristics for RF port 0:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 description Primary downstream channel
```

Cisco IOS CMTS Cable Command Reference

Related Commands

Command	Description
cable primary	Specifies that a wideband channel is a primary wideband channel.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel.
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
ip-address (controller)	Sets the IP address of the Wideband SPA FPGA.
modular-host subslot	Specifies the modular-host line card for Wideband protocol operations.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.
rf-channel frequency	Sets the frequency for each RF channel.
rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address and UDP port for each RF channel.
rf-channel network delay	Configures the network delay for an RF channel.

rf-channel frequency

To configure the frequency of an RF channel on a wideband interface, use the **rf-channel frequency** command in controller configuration mode. To remove the frequency of an RF channel configuration, use the **no** form of this command.

Cisco IOS Releases 12.3(21)BC and 12.2(33)SCA

> **rf-channel** *rf-port* **frequency** *freq*

> **no rf-channel** *rf-port* **frequency**

Cisco IOS Releases 12.3(23)BC and 12.2(33)SCB

> **rf-channel** *rf-port* **frequency** *freq* [**annex** {**A** | **B**} **modulation** {**64** | **256**}
>   [**interleave-depth** {**8** | **12** | **16** | **32** | **64** | **128**}]]

> **no rf-channel** *rf-port* **frequency**

Syntax Description		
	rf-port	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command (see the Usage Guidelines section).
	freq	Sets the center frequency for the RF channel. Allowed range is 55000000 to 1050000000 MHz.
	annex {**A**|**B**}	Specifies the MPEG framing format for each RF channel: • **A**–Annex A. The downstream is compatible with the European MPEG framing format specified in ITU-TJ.83 Annex A. • **B**–Annex B. The downstream is compatible with the North American MPEG framing format specified in ITU-TJ.83 Annex B.
	modulation {**64**|**256**}	Specifies the modulation rate for each RF channel: • **64**–64-QAM • **256**–256-QAM
	interleave-depth{**8** | **12** | **16** | **32** | **64** |*128*}	Indicates the downstream interleave depth. The default value is 32.

Command Default   No default RF channel configuration values are set for frequency, annex, and modulation.

Command Modes   Controller configuration (config-controller)

Command History	Release	Modification
	12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
	12.3(23)BC	The following keyword options were added: • **annex** • **modulation** • **interleave-depth**
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. The **annex**, **modulation**, and **interleave-depth** keyword options are not supported.
	12.2(33)SCB	The **annex**, **modulation**, and **interleave-depth** keyword options are supported.

Usage Guidelines

Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SCA

This command configures the frequency for an RF channel on a Wideband SPA.

The Cisco uBR10012 router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels depending on how the SPA is configured with the **annex modulation** command. For annex A and 256 QAM, each Wideband SPA supports up to 18 RF channels. For all other cases, the SPA supports up to 24 RF channels.

Note   In Cisco IOS 12.3(21)BC and 12.3(21a)BC3 releases, **annex** and **modulation** parameters were set globally for each SPA using the **annex modulation** command.
Beginning in Cisco IOS Release 12.3(23)BC, annex and modulation values are set for each RF channel using the **rf-channel frequency** command. The **annex modulation** command is obsolete.

Cisco IOS Releases 12.3(23)BC and 12.2(33)SCB

This command configures the frequency for an RF channel on a Wideband SPA. The Cisco uBR10012 router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels. For annex A and 256 QAM, each Wideband SPA supports up to 18 RF channels at full rate. For all other cases, the SPA supports up to 24 RF channels.

For each RF channel, use the **rf-channel frequency** command in controller configuration mode to configure RF-channel characteristics. For Cisco IOS Release 12.3(21)BC, for each RF channel (*rf-port*), the frequency option *must be configured* with the **rf-channel frequency** command.

Uniqueness of frequency is required for all cable downstream channels on all cable interfaces and all Wideband SPAs on the CMTS.

Note   Be certain to verify that the RF channel values set with **rf-channel frequency** *match the values configured for the QAM outputs on the edge QAM device*.The frequency value must match. If the value does not match, the Wideband SPA will not successfully communicate with the edge QAM device.

Cisco IOS Release 12.2(33)SCE

In Cisco IOS Release 12.2(33)SCE and later, changing the frequency of a single RF channel in a controller will change the frequency of all RF channels in that controller. In the event of the frequency change, all DOCSIS 3.0 cable modems will start re-registering in downstream partial service mode (p-online).

Examples   The following example shows how to configure RF channel frequency for RF port 0:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 frequency 699000000 annex A modulation 256
interleave-depth 64
```

Related Commands

Command	Description
cable primary	Specifies that a wideband channel is a primary wideband channel.
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
rf-channel description	Specifies the description for each RF channel.
rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address and UDP port for each RF channel.
rf-channel network-delay	Configure the network delay for an RF channel.

rf-channel ip-address mac-address udp-port

To configure the IP address, MAC address, UDP port and DEPI remote ID of an RF channel on a Wideband SPA, use the **rf-channel ip-address mac-address udp-port** command in controller configuration mode. To remove the IP address, MAC address, UDP port and DEPI remote ID configuration of an RF channel, use the **no** form of this command.

Cisco IOS Releases 12.3(21)BC and 12.2(33)SCA

> **rf-channel** *rf-port* **ip-address** *ip-address* **mac-address** *mac-address* **udp-port** *portnum*

> **no rf-channel** *rf-port* **ip-address** *ip-address* **mac-address** *mac-address* **udp-port** *portnum*

Cisco IOS Releases 12.3(23)BC and 12.2(33)SCB

> **rf-channel** *rf-port* **ip-address** *ip-address* **mac-address** *mac-address* {**udp-port** *portnum* | **depi-remote-id** *session-id*}

> **no rf-channel** *rf-port* **ip-address** *ip-address* **mac-address** *mac-address* {**udp-port** *portnum* | **depi-remote-id** *session-id*}

Syntax Description		
	rf-port	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command (see the Usage Guidelines section).
	ip-address	Specifies the IP address of the Gigabit Ethernet interface on the edge QAM device for this RF channel.
	mac-address	Specifies the MAC address of the next-hop interface or of the edge QAM device for this RF channel.
	portnum	Specifies the UDP port number for the edge QAM device that will be used for this RF channel. Allowed range is 0 to 65535.
	session-id	Specifies the DEPI remote session ID to be used for encapsulation of frames in DOCSIS-MPT mode.

Command Default   No default RF channel configuration values are set.

Command Modes   Controller configuration (config-controller)

Command History	Release	Modification
	12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
	12.3(23)BC	The **depi-remote-id** keyword option was added.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. The **depi-remote-id** keyword option is not supported.
	12.2(33)SCB	The **depi-remote-id** keyword option is supported.

Usage Guidelines   For each RF channel, use the **rf-channel ip-address mac-address udp-port** command in controller configuration mode to configure RF-channel characteristics.

The Cisco uBR10012 router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels depending on how the SPA is configured with the **annex modulation** command. For annex A and 256 QAM, each Wideband SPA supports up to18 RF channels. For all other cases, the SPA supports up to 24 RF channels.

Note   In the Cisco IOS Release 12.3(21)BC and 12.3(21a)BC3 releases, **annex** and **modulation** parameters were set globally for each SPA using the **annex modulation** command.
Beginning in Cisco IOS Release 12.3(23)BC, annex and modulation values are set for each RF channel using the **rf-channel frequency** command. The **annex modulation** command is obsolete.

For each RF channel (*rf-port*), the following items *must be configured* with **rf-channel ip-address mac-address udp-port** command:

Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SCA

- IP address
- MAC address
- UDP port
- Associated wideband channel (see the **cable rf-channel** command)

Cisco IOS Releases 12.3(23)BC and 12.2(33)SCB

- IP address
- MAC address
- UDP port or DEPI remote ID
- Associated wideband channel (see the **cable rf-channel** command)

The value used for *mac-address* in the *mac-address* argument is as follows:

- If a Gigabit Ethernet router or Layer 3 switch is used between the Wideband SPA and the edge QAM device, the value specified for *mac-address* is the MAC address for the next-hop interface on the router or Layer 3 switch.

- If a Gigabit Ethernet router or Layer 3 switch is not used, the value specified for *mac-address* is the MAC address for the Gigabit Ethernet interface on the edge QAM device.

The UDP port number set for the RF channel allows mapping an input UDP session to a specific QAM output port. Wideband traffic from different Wideband SPAs cannot be mixed on the same QAM output ports.

Note   Be certain to verify that the RF channel values set with **rf-channel frequency** match the values configured for the QAM outputs on the edge QAM device. IP address, MAC address, UDP port, and DEPI remote ID must match. If any of these values do not match, the Wideband SPA will not successfully communicate with the edge QAM device.

Examples   The following example shows how to configure the RF channel IP address, MAC address UDP port and DEPI remote ID characteristics for RF port 0:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
```

```
Router(config-controller)# rf-channel 0 ip-address 192.168.200.30 mac-address
0011-920e-a9ff udp-port 49152
```

Related Commands

Command	Description
cable primary	Specifies that a wideband channel is a primary wideband channel.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel.
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
ip-address (controller)	Sets the IP address of the Wideband SPA FPGA.
modular-host sub-slot	Specifies the modular-host line card for Wideband protocol operations.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.
rf-channel description	Specifies the description for each RF channel.
rf-channel frequency	Sets the frequency for each RF channel.
rf-channel network delay	Configures the network delay for an RF channel.

rf-channel network-delay

To configure the network delay for an RF channel on a Wideband SPA, use the **rf-channel network delay** command in controller configuration mode. To remove the network delay configuration for an RF channel, use the **no** form of this command.

rf-channel *rf-port* **network-delay** *delay* [**sampling-rate** *rate*]

no rf-channel *rf-port* **network-delay** *delay* [**sampling-rate** *rate*]

Syntax Description

rf-port	RF channel physical port on the Wideband SPA FPGA. The allowed range is from 0 to 23. The valid values for *rf-port* depend on the configuration set with the **annex modulation** command (see the Usage Guidelines section).
delay	Converged Interconnect Network (CIN) delay. The default value is 550 us. The allowed range is from 0 to 3000 us. The *delay* value **auto** determines the delay through DEPI Latency Measurement (DLM) packets.
sampling-rate	(Optional) Specifies how often the DLM is sent. The allowed range is from 1 to 500 sec. The default value is 10 sec. This option is available only when the *delay* value is set to auto.
rate	Sampling-rate value.

Command Default   No default RF channel network delay configuration values are set.

Command Modes   Controller configuration (config-controller)

Command History

Release	Modification
12.3(23)BC	This command was introduced for the Cisco uBR10012 universal broadband router.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
12.2(33)SCC	This command was modified to include **sampling-rate** *rate* to specify how often the DLM is sent.

Usage Guidelines   The Cisco uBR10012 universal broadband router supports two Wideband SPAs. Each Wideband SPA supports up to 24 RF channels depending on how the SPA is configured with the **annex modulation** command. For annex A and 256 QAM, each Wideband SPA supports up to18 RF channels. For all other cases, the SPA supports up to 24 RF channels.

Note In Cisco IOS releases 12.3(21) BC and 12.3(21a)BC3, **annex** and **modulation** parameters were set globally for each SPA using the **annex modulation** command.
From Cisco IOS Release 12.3(23)BC onwards, annex and modulation values are set for each RF channel using the **rf-channel frequency** command. The **annex modulation** command is obsolete.

Examples

The following example shows how to configure the RF channel network delay characteristics for RF port 0:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 network-delay 1000
```

The following example shows how to configure the RF channel network delay characteristics for RF port 0 with a sampling-rate of 1sec:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 network-delay auto sampling-rate 1
```

Related Commands

Command	Description
cable primary	Specifies that a wideband channel is a primary wideband channel.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel.
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
ip-address (controller)	Sets the IP address of the Wideband SPA FPGA.
modular-host subslot	Specifies the modular-host line card for Wideband protocol operations.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.
rf-channel description	Specifies the description for each RF channel.
rf-channel frequency	Sets the frequency for each RF channel.
rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address, and UDP port for each RF channel.

rf-channel rf-power

To set the RF power output level on Cisco UBR-MC20X20V and Cisco uBR-MC88V cable interface line cards, use the **rf-channel rf-power** command in controller configuration mode. To reset the RF output power level to its default value, use the **no** form of this command.

rf-channel *rf-port* **rf-power** *power-level*

no rf-channel *rf-port* **rf-power** *power-level*

Syntax Description

rf-port	RF channel physical port on the Wideband SPA FPGA. The valid range is from 0 to 3. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command.
power-level	Desired RF output power level in dBmV. The valid range is dependent on the cable interface line card. The format is XY.Z. By default, .Z is added as .0.

Command Default   None

Command Modes   Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SCC	This command was introduced.
12.2(33)SCD	This command was modified to support configuration of the controller interface on Cisco uBR7246VXR and Cisco uBR7225VXR universal broadband routers.

Usage Guidelines   For the Cisco UBR-MC20X20V cable interface line card, all the channels within a controller must have the same RF power value. When the RF power value is changed on any one channel, the same value is applied to all the channels within the controller. The recommended RF power range depends on the mode of the upconverter. The mode of the upconverter is decided by the highest numbered channel that is enabled.

Note   RF power value outside the recommended RF power range is accepted but is automatically adjusted. If the input value exceeds the recommended RF power range, it is adjusted to a value lower than the upper limit of the range and if it is less than the recommended range, it is adjusted to a value higher than the lower limit of the range. The RF power level can be configured in decimals too.

Table 36 lists the recommended RF power range for different channel settings on the Cisco UBR-MC20X20V line card.

Table 36 **RF Power Range on the Cisco UBR-MC20X20V Line Card**

Upconverter Mode	Channel Setting	Recommended RF Power Range
Single	Only channel 0 is enabled	60.0 to 52.0 dBmV
Dual	Channel 0 is either enabled or disabled. Channel 1 is enabled. Channel 2 and channel 3 are disabled.	56.0 to 48.0 dBmV
Triple	Channel 0, and channel 1 are either enabled or disabled. Channel 2 is enabled and channel 3 is disabled.	54.0 to 46.0 dBmV
Quad	Channels 0, 1, and 2 are either enabled or disabled. Channel 3 is enabled.	52.0 to 44.0 dBmV

Table 37 lists the recommended RF power range for different channel settings on the Cisco uBR-MC88V line card.

Table 37 **RF Power Range on the Cisco uBR-MC88V Line Card**

Upconverter Mode	Channel Setting	Recommended RF Power Range
Single	The RF channel stacking number equals to 1 in this mode. Channel 0 is enabled while the other channels are disabled.	45 to 63 dBmV
Dual	The RF channel stacking number equals to 2 in this mode. Channels 0 and 1 are enabled; channels 2 and 3 are disabled.	48 to 56 dBmV
Triple	The RF channel stacking number equals to 3 in this mode. Channels 0, 1, and 2 are enabled; channel 3 is disabled.	46 to 54 dBmV
Quad	The RF channel stacking number equals to 4. Channels 0, 1, 2, and 3 are enabled.	44 to 52 dBmV

Examples   The following example shows how to configure RF power for RF port 0 in modular-cable controller mode:

```
Router# configure terminal
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# rf-channel 0 rf-power 50.6
```

The following example shows how to configure RF power for RF port 0 in integrated-cable controller mode:

```
Router# configure terminal
```

```
Router(config)# controller integrated-cable 1/0/0
Router(config-controller)# rf-channel 0 rf-power 50.6
```

Related Commands	Command	Description
	cable primary	Specifies that a wideband channel is a primary wideband channel.
	controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
	controller integrated-cable	Enters integrated-cable controller configuration mode.
	rf-channel description	Specifies the description for each RF channel.
	rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address and UDP port for each RF channel.
	rf-channel frequency	Configures the frequency for the RF channel.
	rf-channel network-delay	Configure the network delay for an RF channel.
	rf-channel rf-shutdown	Enables or disables RF output on a Wideband SPA.

rf-channel rf-shutdown

To disable the RF output on a wideband interface, use the **rf-channel rf-shutdown** command in controller configuration mode. To enable the RF output, use the **no** form of this command.

rf-channel *rf-port* **rf-shutdown**

no rf-channel *rf-port* **rf-shutdown**

Syntax Description

rf-port	Specifies the RF channel physical port. Allowed range is from 0 to 3. Valid values for *rf-port* depend on the configuration set with the **annex modulation** command.

Command Default   RF output is disabled.

Command Modes   Controller configuration (config-controller)

Command History

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

Usage Guidelines   Starting with Cisco IOS Release 12.2(33)SCE, when you use the **rf-channel rf-shutdown** command, all DOCSIS 3.0 cable modems associated with the RF channel on a particular wideband interface will go offline and start re-registering in downstream partial service mode (p-online). In Cisco IOS Release 12.2(33)SCD and earlier, cable modems do not go offline while using the **rf-channel rf-shutdown** command.

For muting and unmuting the QAM on the Cisco RFGW-10, use the **rf-channel rf-shutdown** command in the M-CMTS.

Examples   The following example enables RF output on the Cisco wideband SPA:

```
Router# enable
Router# configure terminal
Router(config)# controller integrated-cable 7/1/0
Router(config-controller)# no rf-channel 0 rf-shutdown
```

Related Commands

Command	Description
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
controller integrated-cable	Enters integrated-cable controller configuration mode.

Command	Description
rf-channel network-delay	Configure the network delay for an RF channel.
rf-channel rf-power	Sets the RF power output level on the Cisco UBR-MC20X20V cable interface line card.

rf-channel stacking

To suppress a carrier or mute a radio frequency (RF) channel on the Cisco uBR-MC88V cable interface line card, use the **rf-channel stacking** command in controller configuration mode. To remove the configuration, use the **no** form of this command.

rf-channel stacking *stacking-number*

no rf-channel stacking *stacking-number*

Syntax Description	*stacking-number* RF channel stacking number. The valid range is from 1 to 4. The default value is 4.

Command Default   The RF channel stacking number is set to 4.

Command Modes   Controller configuration (config-controller)

Command History

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

Usage Guidelines   If you change the default stacking number configuration, traffic loss may occur on the active channels. For example, if you change the stacking number from 4 to 2, traffic is interrupted on the RF channels 0 and 1. However, traffic loss does not occur if you do not change the stacking number configuration when shutting down an RF channel using the **rf-channel rf-shutdown** command.

> **Note**   We recommend that you do not change the default stacking number configuration. You can change the default configuration when you want RF diagnostics performed on a particular channel. For example, if you want to perform RF diagnostics on RF channel 2, you need to change the default stacking number configuration to 2 to completely mute this channel.

Examples   The following example shows how to configure the RF channel stacking number for the Cisco uBR-MC88V cable interface line card:

```
Router# configure terminal
Router(config)# controller integrated-cable 5/1
Router(config-controller)# rf-channel stacking 3
```

Related Commands

Command	Description
rf-channel rf-shutdown	Disables the RF output on a Cisco Wideband SPA, or a cable interface line card.

rf-switch auxport enable

To enable the AUX port of the RF switch, use the **rf-switch auxport enable** command in redundancy mode. To disable the AUX port, use the **no** form of this command.

rf-switch auxport enable

no rf-switch auxport

Syntax Description

enable	Enables the Cisco NGRFSW-ADV. In the default configuration, the Cisco NGRFSW-ADV is disabled. When the Cisco NGRFSW-ADV is enabled, the Cisco CMTS router starts polling the Cisco NGRFSW-ADV at a set interval to check its status.

Command Default

The AUX port of the Cisco NGRFSW-ADV is disabled by default.

Command Modes

Redundancy mode (config-red)

Command History

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

Examples

The following example shows how to enable the AUX port of the Cisco NGRFSW-ADV:

```
Router> enable
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# rf-switch auxport enable
```

Associated Features

The **rf-switch auxport enable** command is used to configure the Cisco uBR Advanced RF Switch (NGRFSW-ADV). See Cisco uBR Advanced RF Switch Software Configuration Guide.

Related Commands

Command	Description
linecard-group *id* cable	Assigns the Hot Standby Connection-to-Connection Protocol (HCCP) group to all interfaces on the cable interface line card, or Cisco Broadband Processing Engine.
show redundancy linecard	Displays information about a redundant line card or line card group.

secondary aux

To enable the auxiliary port on the standby PRE1 module, use the **secondary aux** command in redundancy configuration (main-cpu) mode. To disable the auxiliary port, use the **no** form of this command.

secondary aux

no secondary aux

Syntax Description   This command has no keywords or arguments.

Defaults   The auxiliary port on the standby PRE1 module is disabled.

Command Modes   Redundancy configuration, main-cpu mode

Command History

Release	Modification
12.2(11)BC3	This command was introduced for the Cisco uBR10012 router.

Examples   The following example shows how to enable the auxiliary port on the standby PRE1 module.

```
Router# config t
Router(config)# redundancy
Router(config-r)# main-cpu
Router(config-r-mc)# secondary aux
Router(config-r-mc)# exit
Router(config-f)# exit
Router(config)#
```

Related Commands

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode, so that you can configure the synchronization of the active and standby Performance Routing Engine (PRE1) modules.
redundancy	Configures the synchronization of system files between the active and standby PRE1 modules.
redundancy force-failover main-cpu	Forces a manual switchover between the active and standby PRE1 modules.

service-class (cmts-tag)

To configure the specified service class name for the CMTS tag, use the **service-class** command in the cmts-tag configuration mode. To remove the configured service class name from the CMTS tag, use the **no** form of this command.

[**exclude**] **service-class** *service-class-name*

no service-class *service-class-name*

Syntax Description

exclude	(Optional) Configures the CMTS tag to exclude the specified service class name.
service-class-name	Service class name with matching rule

Command Default   No default behavior or values.

Command Modes   CMTS tag mode (cmts-tag)

Command History

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

Examples   The following example shows how to configure the specified service class name for the CMTS tag using the **service-class** command:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# service-class uBR
```

Related Commands

Command	Description
cable load-balance docsis-group	To configure a DOCSIS load balancing group on the CMTS.
show cable load-balance docsis-group	To display real-time configuration, statistical and operational information for load balancing operations on the router.
cable tag	To configure a tag for a DOCSIS load balancing group on the CMTS.

service-class (enforce-rule)

To identify a particular service class for cable modem monitoring in an enforce-rule, use the **service-class (enforce-rule)** command in enforce-rule configuration mode. To remove the service class from the enforce-rule, use the **no** form of this command.

service-class {**enforced** | **registered**} *name*

no service-class {**enforced** | **registered**} *name*

<table>
<tr><td rowspan="3">**Syntax Description**</td><td>**enforced**</td><td>Specifies an enforced service class.</td></tr>
<tr><td>**registered**</td><td>Specifies enforcing of QoS profiles for the registered service class.</td></tr>
<tr><td>*name*</td><td>Specifies the name of the service class.</td></tr>
</table>

Command Default   No default behavior or values

Command Modes   Enforce-rule configuration (enforce-rule)

<table>
<tr><td rowspan="3">**Command History**</td><td>**Release**</td><td>**Modification**</td></tr>
<tr><td>12.3(9a)BC</td><td>This command was introduced.</td></tr>
<tr><td>12.2(33)SCA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.</td></tr>
</table>

Usage Guidelines   The **service-class (enforce-rule)** command allows operators to identify the name of the initial registered service class for a CM in an enforce-rule, and also the name of a new service class to be enforced if the CM violates its registered service parameters.

Examples   The following example shows specification of the enforced service class called "test" in an enforce-rule:

```
Router(enforce-rule)# service-class enforced test
```

<table>
<tr><td rowspan="5">**Related Commands**</td><td>**Command**</td><td>**Description**</td></tr>
<tr><td>**cable qos enforce-rule**</td><td>Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.</td></tr>
<tr><td>**debug cable subscriber-monitoring**</td><td>Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.</td></tr>
<tr><td>**duration**</td><td>Specifies the time period and sample rate to be used for monitoring subscribers.</td></tr>
<tr><td>**enabled (enforce-rule)**</td><td>Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.</td></tr>
</table>

Command	Description
monitoring-basics	Specifies the type of monitoring desired for subscriber traffic management on a Cisco CMTS router.
peak-time1	Specifies peak and offpeak monitoring times on a Cisco CMTS router.
qos-profile registered	Specifies the registered QoS profile that should be used for this enforce-rule.
show cable qos enforce-rule	Displays the QoS enforce-rules that are currently defined.
show cable subscriber-usage	Displays subscribers who are violating their registered QoS profiles.

service divert-rate-limit

> ✎
>
> **Note**   Effective with Cisco IOS Release 12.2(33)SCB, the **service divert-rate-limit** *fib-rp-glean* command is replaced on the WAN-side by the **service divert-rate-limit ip** *fib-rp-glean* command. See the **service divert-rate-limit ip** command for more information. The **service divert-rate-limit** *fib-rp-glean* command is replaced on the WAN-side non-IP by **service divert-rate-limit non-ip** *fib-rpf-glean* command. See the **service divert-rate-limit non-ip** command for more information. For cable-side DRL configuration, see the **cable divert-rate-limit** command.

To configure PXF Divert-Rate-Limit, use the **service divert-rate-limit** command in global configuration mode. To reset this feature to the default parameters, use the **no** form of this command.

service divert-rate-limit *divert-code rate* [**limit** *limit*]

no service divert-rate-limit *divert-code*

Syntax Description	*divert-code rate*	Configures the PXF Divert-Rate-Limit for the any of the following packets:
		• fwd-glean—Packets that hit a glean adjacency in the FIB.
		• rpf-glean—Packets that hit a glean adjacency during the RPF check.
		The range is from 1 to 255 packet-per-second.
		The default rate is 20 packets-per-second.
	limit *limit*	(Optional) Sets the limit for the number of packets that will be diverted in an initial burst of packets.
		The range is from 4 to 255 packets.
		The default limit is 5 packets.
		✎ **Note** Setting the limit has a limited effect on the behavior of the algorithm, so this part of the CLI is hidden.

Defaults   Divert-Rate-Limit contains the following default behavior and values:

- Divert-Rate-Limit is always active.
- The default rate is 20 packets-per-second.
- The default limit is 5 packets.

Command Modes   Global configuration (config)

Command History

12.3(17a)BC	The command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
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 replaced by the **service divert-rate-limit ip** *fib-rp-glean* command and **service divert-rate-limit non-ip** *fib-rpf-glean* command.

Usage Guidelines

The **service divert-rate-limit** command is used to configure the PXF Divert-Rate-Limit for fwd-glean and rpf-glean packets in order to identify packet streams that will cause congestion of the FP-to-RP interface.

Examples

The following example shows how to configure rate-limiting for fib-rp-glean, with a rate of 10 packets-per-second and a limit of 20 packets:

```
Router(config)# service divert-rate-limit fib-rp-glean 10 limit 20
```

The following example shows how to return rate-limiting for fib-rp-glean to the default values:

```
Router(config)# no service divert-rate-limit fib-rp-glean
```

Pass and fail counters are kept for fwd-glean, rpf-glean, and cable-ARP packets. To show the statistics for the pass and fail counter, use the **show pxf cpu statistics drl** command:

```
Router(config-if)# show pxf cpu statistics drl
   Divert-Rate-Limit statistics
     code        total          diverted          dropped
   fib_rpf_glean  500            59                441
   fib_rp_glean   500            54                446
   arp_filter     0             0                 0
```

Note The arp_filter stats shown above are global stats for PXF ARP Filtering. These stats cannot be cleared by the CLI. However, they will reset to zero upon reload.

Packets dropped by Divert-Rate-Limit and the ARP Filter will be recorded in the regular PXF drop statistics:

```
Router(config-if)# show pxf cpu statistics drop c5/0/0
   FP drop statistics for Cable5/0/0
                            packets          bytes
     vcci undefined         0                0
   vcci C
     ...
     divert_rate_limit      441              28224
     arp_filter_reply       0                0
     arp_filter_request     0                0
```

Related Commands

Command	Description
show cable arp-filter	Displays the total number of Address Resolution Protocol (ARP) offenders.

service divert-rate-limit ip

To set DRL rate and limit for WAN-side IP packet streams, use the **service divert-rate-limit ip** command in global configuration mode. To reset the *rate* and *limit* to the default values for all IP divert-codes, use the **no** form of this command. Using **no service divert-rate-limit ip** *divert-code* will reset *rate* and *limit* to the default values for the specified divert code.

> **service divert-rate-limit ip** *divert-code* **rate** *rate* **limit** *limit*

> **no service divert-rate-limit ip**

Syntax Description

divert code	Specifies the applicable divert code.
rate	Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second.
	For WAN-side IP packets, the default rate is 4000 packets per second
limit	Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets.
	For WAN-side IP packets, the default limit is 4000 packets.

Command Default   For WAN-side IP packet streams, the default rate is 4000 packets per second and default limit is 4000 packets. These defaults apply to each uniquely identified IP packet stream.

Command Modes   Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
	The **service divert-rate-limit ip** *fib-rp-glean* command is the WAN-side replacement for the **service divert-rate limit** *fib-rp-glean* command.

Usage Guidelines   You can configure a rate and limit for a particular IP divert-code for WAN-side IP packets. However, each IP packet-stream is uniquely identified (using a hash of the VRF, the IP source address, and the divert-code), and then packets in that stream are sent through a rate-limiter with the configured rate and limit.

Examples   The following example shows how to set the rate and limit for the specified divert code:

```
Router(config)# service divert-rate-limit ip fib-rp-glean rate 1 limit 4
```

Related Commands

Command	Description
service divert-rate-limit non-ip	This command configures DRL for WAN-side non-IP packet streams.
service divert-rate-limit trusted-site	This command adds entries to the trusted site list.

service divert-rate-limit ipv6

To set the divert rate limit (DRL) rate and limit for WAN-side IPv6 packet streams, use the **service divert-rate-limit ipv6** command in global configuration mode.

service divert-rate-limit ipv6 *divert-code* **rate** *rate* **limit** *limit*

no service divert-rate-limit ipv6

Syntax Description		
divert-code	Specifies the applicable divert code.	
rate	Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second.	
	For WAN-side IPv6 packets, the default rate is 4000 packets per second.	
limit	Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets.	
	For WAN-side IPv6 packets, the default limit is 4000 packets.	

Command Default   For WAN-side IPv6 packet streams, the default rate is 4000 packets per second and default limit is 4000 packets.

Command Modes   Global configuration (config)

Command History	Release	Modification
	12.2(33)SCE	This command was introduced.

Usage Guidelines   You can configure rate and limit for a particular IPv6 divert-code for WAN-side IP packets. However, each IP packet-stream is uniquely identified (using a hash of the VRF, the IP source address, and the divert-code), and then packets in that stream are sent through a rate-limiter with the configured rate and limit.

This command is supported only on PRE4.

Use the **diversion** option of the **show pxf cpu statistics** command to troubleshoot the divert code, before configuring the DRL.

To configure the correct divert code, refer to the list of divert codes.

Table 38   List of divert codes

Divert Code	Description
6pe_dst_linklocal	6PE dst linklocal
6pe_dst_mcast	6PE dst multicast
6pe_ttl	6PE ttl
icmpv6	IPv6 ICMP

Divert Code	Description
ipv6_cable_filter_ds	ipv6 cable filter ds
ipv6_dhcp_ucast	IPv6 unicast DHCP
ipv6_hopopts	IPv6 HopOpts
ipv6_lng_ext_hdr	IPv6 long extension hdr
ipv6_mcast_rsvd	IPv6 multicast
ipv6_nd_na_mcast	IPv6 ND NA (multicast)
ipv6_nd_na_ucast	IPv6 ND NA (unicast)
ipv6_nd_ns_mcast	IPv6 ND NS (multicast)
ipv6_nd_ns_ucast	IPv6 ND NS (unicast)
ipv6_nd_rs_mcast	IPv6 ND RS (multicast)
ipv6_rp_dest	IPv6 receive adjacency
ipv6_rp_glean	IPv6 glean adjacency
ipv6_rp_pbr	IPv6 RP PBR
ipv6_rp_punt	IPv6 punt adjacency
ipv6_src_linklocal	IPv6 SRC LinkLocal
ipv6_src_ver_lq_req	IPv6 src ver leasequery request
ipv6_src_ver_mac_req	IPv6 src ver MAC request

Note To reset the *rate* and *limit* to the default values for all IPv6 divert-codes, use the **no** form of this command. Using **no service divert-rate-limit ipv6** *divert-code* will reset *rate* and *limit* to the default values for the specified divert code.

Examples The following example shows how to set the rate and limit for the specified divert code:

```
Router(config)# service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10
Router(config)#
```

Related Commands

Command	Description
service divert-rate-limit trusted-site	Adds IPv4-specific entries to the trusted site list.
service divert-rate-limit non-ip	Configures DRL for WAN-side non-IP packet streams.
service divert-rate-limit trusted-site-ipv6	Adds IPv6-specific entries to the trusted site list.
show pxf cpu statistics	Displays Parallel eXpress Forwarding (PXF) CPU statistics.

Cisco IOS CMTS Cable Command Reference

service divert-rate-limit ip trusted-site

To add entries to the trusted site list, use the **service divert-rate-limit ip trusted-site** command in the global configuration mode. To remove all entries from the trusted site list, use the **no** form of this command.

> **service divert-rate-limit ip trusted-site** *ip-address* **mask** *ip-address* **tos** *tos-value* **mask** *tos-mask* **vrf** *vrf-name*

> **no service divert-rate-limit ip trusted-site** *ip-address* **mask** *ip-address* **tos** *tos-value* **mask** *tos-mask* **vrf** *vrf-name*

Syntax Description		
ip-address	Specifies the source IP address that should be matched.	
	Example: 64.12.13.0	
mask *ip-address*	The mask to apply to the source IP address of the packet before testing if it matches. There are no restrictions on the mask value.	
	Example: 255.255.0.255	
tos *tos-value*	The ToS value of the trusted site. There are no restrictions on the tos_value. Example: 0xD0	
mask *tos-mask*	The mask to apply to the IP ToS value and the trusted-site tos_value before testing if it matches. There are no restrictions on the tos_mask value.	
	Example: 0xF3	
	✎ **Note** The ToS value can be wild-carded by setting the tos_mask to 0x00	
vrf *vrf-name*	The VRF that this trusted site applies to.	
	For the global VRF, use the **global** keyword. To apply the trusted-site to all VRFs (including the global VRF), hit enter after specifying the *tos-mask*.	
	If a non-existent VRF is specified, the table entry is filled, but the information is not written to toaster memory. If the specified VRF is subsequently created, the information is written to toaster at that time.	

Command Default   No default behavior or values.

Command Modes   Global configuration (config)

Command History

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

Usage Guidelines   The **service divert-rate-limit ip trusted-site** command is used to configure trusted site list that contains a source IP address and mask, IP ToS value and mask, and a VRF. If no IP address is specified, the entire trusted site list is cleared. The trusted site list contains a source IP address and mask, IP ToS value and mask, and a VRF. The trusted site list applies only to WAN-IP IPv4 packets. There is a limitation of four trusted sites.

Examples   The following example shows how to configure trusted site list:

```
Router(config)# service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255
      tos 0xD0 mask 0xF3 vrf name1
```

Related Commands

Command	Description
service divert-rate-limit non-ip	This command sets and limit default values for the specified divert code.

service divert-rate-limit trusted-site-ipv6

To add IPv6-specific entries to the trusted site list, use the **service divert-rate-limit trusted-site-ipv6** command in the global configuration mode. To remove all entries from the trusted site list, use the **no** form of this command.

service divert-rate-limit trusted-site-ipv6 *ip-address* **traffic-class** *tc_value* **mask** *tc-mask* [**global** | **vrf** vrf-name]

no service divert-rate-limit trusted-site-ipv6

Syntax Description		
ip-address	The source IPv6 address that should be matched.
traffic-class *tc_value*	The 8-bit traffic-class of the trusted site. There are no restrictions on the *tc_value*. Example: 0xD0
mask *tc-mask*	The mask to apply to the packet traffic-class and the trusted-site *tc_value* before testing if it matches. There are no restrictions on the *tc_mask* value. Example: 0xF3
vrf vrf-name	The virtual route forwarding (VRF) instance to which this trusted site is being applied. For the global VRF, use the **global** keyword. To apply the trusted-site to all VRFs (including the global VRF), hit enter after specifying the *tc-mask*.

Command Default   Disabled

Command Modes   Global configuration (config)

Command History

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

Usage Guidelines   This command is used to configure trusted site list that contains an IPv6 source-address/prefix-length, a traffic-class value & mask, and a VRF. There is a limitation of four trusted sites.

Note   The **no** form of the command is used to remove all entries from the trusted site list. To remove a specific entry you should specify the matching source IP address. For example: **no service divert-rate-limit trusted-site-ipv6** *ip-address* **traffic-class** *tc_value* **mask** *tc-mask* [**global** | **vrf** vrf-name].

Examples   The following example shows how to configure IPv6 trusted site list:

```
Router(config)# service divert-rate-limit trusted-site-ipv6
2001:420:3800:800:21F:29FF::1/128 traffic-class 0x3 mask 0xFF global
Router(config)#
```

Related Commands	Command	Description
	show pxf cpu statistics drl us-cable	Displays the number of upstream cable packets that are dropped from the CMTS.
	show pxf cpu statistics drl ipv6	Verifies the drop counters for WAN-IPv6 packets.
	show pxf cpu statistics drl ipv4	Verifies the drop counters for WAN-IPv4 packets.

service divert-rate-limit non-ip

To set DRL for WAN-side non-IP packet streams, use the **service divert-rate-limit non-ip** command in global configuration mode. To reset the *rate* and *limit* to the default values for all non-IP divert-codes, use the **no** form of this command. Using **no service divert-rate-limit non-ip** *divert-code* will reset *rate* and *limit* to the default values for the specified divert-code.

service divert-rate-limit non-ip *divert-code* **rate** *rate* **limit** *limit*

no service divert-rate-limit non-ip

Syntax Description		
	divert-code	Specifies the applicable divert code.
	rate	Specifies the rate in packets per second. Minimum rate is one packet per second. Maximum rate is 65535 packets per second.
		For WAN-side non-IP packets, the default rate is 2000 packets per second.
	limit	Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets.
		For WAN-side non-IP packets, the default limit is 2000 packets.

Command Default For WAN-side non-IP packets, the default rate is 2000 packets per second and default limit is 2000 packets.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCB	This command was introduced.
		The **service divert-rate-limit non-ip** *fib-rpf-glean* command is the WAN-side non-IP replacement for the **service divert-rate limit** *fib-rpf-glean* command.

Usage Guidelines You can configure a rate and limit for a particular non-IP divert-code, and all packets arriving with that divert-code are sent through a single rate-limiter with the configured rate and limit. but the explanation is fairly straightforward: there is a single rate-limiter for each non-IP divert-code. No attempt is made to uniquely identify the source of the attacking packet stream.

Examples The following example shows how to set and limit default values for the specified divert code:

```
Router(config)# service divert-rate-limit non-ip fib-rpf-glean rate 5 limit 25
```

Related Commands

Command	Description
service divert-rate-limit ip	This command configures DRL rate and limit for WAN-side IP packet streams.

service divert-rate-limit trusted-site

To add entries to the trusted site list, use the **service divert-rate-limit trusted-site** command in the global configuration mode. To remove all entries from the trusted site list, use the **no** form of this command.

> **service divert-rate-limit trusted-site** *ip-address mask-ip-address* **tos** *tos-value* **mask** *tos-mask* [**global** | **vrf** *vrf-name*]

> **no service divert-rate-limit trusted-site**

Syntax Description

ip-address	Specifies the source IP address that should be matched.
	Example: 64.12.13.0
mask *ip-address*	The mask to apply to the source IP address of the packet before testing if it matches. There are no restrictions on the mask value.
	Example: 255.255.0.255
tos *tos-value*	The ToS value of the trusted site. There are no restrictions on the tos_value. Example: 0xD0
mask *tos-mask*	The mask to apply to the IP ToS value and the trusted-site tos_value before testing if it matches. There are no restrictions on the tos_mask value.
	Example: 0xF3
	✎
	Note The ToS value can be wild-carded by setting the tos_mask to 0x00
vrf *vrf-name*	The VRF that this trusted site applies to.
	For the global VRF, use the **global** keyword. To apply the trusted-site to all VRFs (including the global VRF), hit enter after specifying the *tos-mask*.
	If a non-existent VRF is specified, the table entry is filled, but the information is not written to toaster memory. If the specified VRF is subsequently created, the information is written to toaster at that time.

Command Default   No default behavior or values.

Command Modes   Global configuration (config)

Command History

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

<u>**Usage Guidelines**</u>   The **service divert-rate-limit ip trusted-site** command is used to configure trusted site list that contains a source IP address and mask, IP ToS value and mask, and a VRF. The trusted site list contains a source IP address and mask, IP ToS value and mask, and a VRF. The trusted site list applies only to WAN-IP IPv4 packets. There is a limitation of four trusted sites.

To remove specified entry from the trusted site list, use **no service divert-rate-limit trusted-site** *ip-address* **mask** *ip-address* **tos** *tos-value* **mask** *tos-mask* [**global** | **vrf** *vrf-name*]. If no IP address is specified, the entire trusted site list is cleared.

<u>**Examples**</u>   The following example shows how to configure trusted site list:

```
Router(config)# service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255
        tos 0xD0 mask 0xF3 vrf name1
```

<u>**Related Commands**</u>

Command	Description
service divert-rate-limit non-ip	This command sets and limit default values for the specified divert code.

Cisco IOS CMTS Cable Command Reference ■

service instance

To configure an Ethernet service instance, use the **service instance** command in Layer 2 VPN configuration mode. To disable this configuration, use the **no** form of this command.

service instance *id service-type*

no service instance *id service-type*

Syntax Description

id	Service instance ID.
service-type	Service type for the instance.

Command Default   None

Command Modes   Layer 2 VPN configuration (config-l2vpn)

Command History

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

Usage Guidelines   You must provision a Multiprotocol Label Switching (MPLS) pseudowire before configuring an Ethernet service instance in Layer 2 VPN configuration mode.

Examples   The following example shows how to configure an Ethernet service instance on a Cisco uBR10012 router:

```
Router # configure terminal
Router(config) # cable l2vpn 001e.6bfb.0f9e customer2
Router(config-l2vpn) # service instance 7000 ethernet
```

Related Commands

Command	Description
cable l2-vpn-service xconnect	Enables the use of Layer 2 tunnels based on an MPLS pseudowire.

service udp-small-servers max-servers no-limit

To enable use of minor servers that use the UDP protocol (such as ToD, echo, chargen, and discard), use the **service udp-small-servers max-servers no-limit** command in global configuration mode. To remove this configuration, use the **no** form of this command.

> **service udp-small-servers max-servers no-limit**

> **no service udp-small-servers max-servers no-limit**

Command Default   DHCP or ToD servers are not configured by default.

Command Modes   Global configuration

Command History

Release	Modification
12.1 EC	Command support introduced on the Cisco CMTS.

Usage Guidelines   Disabling the ping option can speed up address assignment when a large number of modems are trying to connect at the same time. However, disabling the ping option can also result in duplicate IP addresses being assigned if users assign unauthorized static IP addresses to their CPE devices.

Examples   The following example illustrates configuration of this command:

```
Router# configure terminal
Router(config)# service udp-small-servers max-servers no-limit
Router(config)#
```

The following example shows a typical ToD server configuration:

```
service udp-small-servers max-servers no-limit
cable time-server
```

These are the only commands required to enable the ToD server.

Usage Guidelines   The **max-servers no-limit** option allows a large number of cable modems to obtain the ToD server at one time, in the event that a cable or power failure forces many cable modems offline. When the problem has been resolved, the cable modems can quickly reconnect.

✎
Note   Do not disable the minor UDP servers if you are also enabling the other DHCP or TFTP servers.

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

- *Filtering Cable DHCP Lease Queries on the Cisco CMTS*
- *DHCP and Time-of-Day Services on the Cisco CMTS*

Cisco IOS CMTS Cable Command Reference ■

Related Commands	Command	Description
	cable dhcp-giaddr policy	Sets the DHCP *giaddr* field of DHCP request packets to the primary address for cable modems and the secondary address for CPE devices, allowing the use of separate address pools for the different clients.
	cable dhcp-parse option	Enables the parsing of certain DHCP options.
	cable helper-address	Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or subinterface.
	ip dhcp ping packet 0	Instructs the DHCP server to assign an IP address from its pool without first sending an ICMP ping to test whether a client is already currently using that IP address.
	ip dhcp relay information option	Configures the DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
	ip dhcp smart-relay	Enables the DHCP relay agent on the CMTS to automatically switch a cable modem or CPE device to a secondary DHCP server or address pool if the primary DHCP server does not respond to three successive requests.

service-class

To create a DOCSIS configuration file that specifies the quality-of-service (QoS) service-class options for the CM configuration file, use the **service-class** command in cable config-file configuration mode. To disable the specification, use the **no** form of this command.

> **service-class** *class* {**guaranteed-upstream** *us-bandwidth* **max-burst** *burst-size* **max-downstream** *max-dsbandwidth* **max-upstream** *max-usbandwidth* **priority** *priority-num* **privacy**}

> **no service-class**

Syntax Description

class	Specifies service class number. Valid range is 1 to 16. Default value is 1.
guaranteed-upstream *us-bandwidth*	Specifies the guaranteed upstream bandwidth in kbps. Valid range for *us-bandwidth* is 0 to 100000 kbps. Default value is 0.
max-burst *burst-size*	Specifies the maximum upstream burst size in bytes. Valid range for *burst-size is 0 to 65535. Default value is 0, unlimited burst* length. 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 1500 bytes prevents upstream transmission of large Ethernet frames for any modem or CMTS not implementing fragmentation (an optional feature in DOCSIS 1.0).
max-downstream *max-dsbandwidth*	Specifies the downstream bandwidth in kbps. Valid range for *max-dsbandwidth* is 0 to 100000 kbps. Default value is 0.
max-upstream *max-usbandwidth*	Specifies the upstream bandwidth in kbps. Valid range for *max-usbandwidth* is 0 to 100000 kbps. Default value is 0.
priority *priority-num*	Specifies the service class priority. Valid range for *priority-num* is 0 to 7, where 7 is the highest-priority service-class setting.
privacy	Enables baseline privacy interface (BPI).

Command Default

Service-class is not set by default. A CM cannot register on a Cisco CMTS unless at least one parameter in a service class is specified.

Command Modes

Cable config-file (config-file)

Command History

Release	Modification
12.1(2)EC1	This command was introduced.
12.2(4)BC1	This command was integrated into Cisco IOS Release 12.2(4)BC1.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines   Default values can be used only if **service-class** *class* is specified. A single configuration file should not contain multiple service-class ID numbers. Thus, all parameters should be set using a single service-class ID. However, different configuration files can reuse the same service-class ID.

> **Note**   To enable Baseline Privacy Interface (BPI) operations on the cable command, you must specify both the **service-class privacy** and **privacy** commands for the cable modem's DOCSIS configuration file.

Examples   The following example shows how to specify the **service-class** command for a DOCSIS configuration file:

```
router(config)# cable config-file upgrade.cm
router(config-file)# service-class 1 priority 0
router(config-file)# service-class 1 max-upstream 3247
router(config-file)# service-class 1 max-downstream 10000
router(config-file)# service-class 1 max-burst 1600
router(config-file)# service-class 1 privacy
router(config-file)# privacy
router(config-file)# exit
```

Related Commands

Command	Description
cable config-file	Creates a DOCSIS configuration file and enters configuration file mode.
access-denied	Disables access to the network.
channel-id	Specifies upstream channel ID.
cpe max	Specifies CPE information.
download	Specifies download information for the configuration file.
frequency	Specifies downstream frequency.
option	Specifies vendor-specific information fields and other config-file options.
privacy	Specifies privacy options for baseline privacy images.
snmp manager	Specifies SNMP options.
timestamp	Enables time-stamp generation.

service-type-id

To add a service type ID that is compared against the cable modem provisioned service type ID, to determine an appropriate restricted load balancing group (RLBG), use the **service-type-id** command in the config-lb-group configuration mode. To remove the service type ID, use the **no** form of this command.

> **service-type-id** *string*

> **no service-type-id** *string*

Syntax Description

string	Identifier of the service type that gets added to the load balancing group.

Command Default   No default behavior or values.

Command Modes   DOCSIS load balancing group mode (config-lb-group)

Command History

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

Usage Guidelines   You can use the **service-type-id** command to add a service type ID only to a RLBG.

Examples   The following example shows how to add a service type ID on the CMTS, using the **service-type-id** command.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# restricted
Router(config-lb-group)# service-type-id commercial
Router(config-lb-group)# no service-type-id commercial
Router(config-lb-group)#
```

Related Commands

Command	Description
cable load-balance docsis-group	Configures a DOCSIS load balancing group on the CMTS.
show cable load-balance docsis-group	Displays real-time configuration, statistical, and operational information for load balancing operations on the router.

service-type-id (cmts-tag)

To configure the specified service type ID for the CMTS tag, use the **service-type-id** command in the cmts-tag configuration mode. To remove the service type ID, use the **no** form of this command.

[**exclude**] **service-type-id** *service-type-id*

no service-type-id *service-type-id*

Syntax Description	exclude	(Optional) Configures the CMTS tag to exclude the specified service type ID.
	service-type-id	Sets a matching rule with the specified service type ID.

Command Default   No default behavior or values.

Command Modes   CMTS tag mode (cmts-tag)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.

Examples

The following example shows how to configure the specified service type ID for the CMTS tag using the **service-type-id** command:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# service-type-id commercial
```

Related Commands	Command	Description
	cable load-balance docsis-group	To configure a DOCSIS load balancing group on the CMTS.
	show cable load-balance docsis-group	To display real-time configuration, statistical and operational information for load balancing operations on the router.
	cable tag	To configure a tag for a DOCSIS load balancing group on the CMTS.

session-range

To identify the multicast QoS group session range, use the **session-range** command in multicast QoS configuration mode. To disable the QoS group session range, use the **no** form of this command.

session-range *ip-address ip-mask*

no session-range *ip-address ip-mask*

Syntax Description

ip-address	Specifies the IP address of the multicast QoS group.
ip-mask	Specifies the IP mask of the multicast QoS group.

Command Default   A session range IP address and IP mask are not defined for a specific multicast QoS group.

Command Modes   Multicast QoS configuration (config-mqos)

Command History

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

Usage Guidelines   Use the **session-range** command to configure the session range to specify the number of multicast sessions to be admitted on a particular service flow. CMTS does not admit new sessions (no forwarding) if the current number of sessions has reached the defined limit, and waits until a session ends to free up a slot for new sessions. You can configure multiple session ranges.

Examples   The following example defines a session range IP address and IP mask using the **session-range** command:

```
Router(config)# cable multicast qos group 20 priority 55 global
Router(config-mqos)# session-range 224.10.10.01 255.255.255.254
```

Related Commands

Command	Description
cable multicast qos group	Specifies and configures a cable multicast QoS group.
show interface bundle multicast-sessions	Displays multicast session information for a specific virtual cable bundle.
show interface cable multicast-sessions	Displays multicast session information for a specific cable interface.

set clock

To set the system clock on the Cisco CMTS, use the **set clock** command in global configuration mode.

    set clock *time-date*

Syntax Description	*time-date* Time and date for which to set the clock on the Cisco CMTS.

Command Default   Time-of-Day, DHCP, and TFTP server configuration not defined on the Cisco CMTS by default.

Command Modes   Global configuration

Command History

Release	Modification
12.0(4)XI	This feature was introduced for the Cisco uBR7200 series routers.
12.1(5)EC	This feature was supported on the Cisco uBR7100 series routers.
12.2(4)BC1	This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms.

Usage Guidelines   To supply an accurate clock, the system clock on the Cisco CMTS should be configured for the correct time, either by using the **set clock** command or by configuring the Cisco CMTS to act as a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) client.

For proper operation of the DOCSIS network, especially a DOCSIS 1.1 network using BPI+ encryption and authentication, the system clock on the Cisco CMTS must be set accurately. You can achieve this by manually using the **set clock** command, or by configuring the CMTS to use either the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP).

For additional information about the set clock command, refer to the following documents on Cisco.com:

- *Time-of-Day Server for the Cisco CMTS*
- *DHCP, ToD, and TFTP Services for the Cisco Cable Modem Termination System*

Related Commands

Command	Description
cable dhcp-giaddr policy	Sets the DHCP *giaddr* field of DHCP request packets to the primary address for cable modems and the secondary address for CPE devices, allowing the use of separate address pools for the different clients.
cable dhcp-parse option	Enables the parsing of certain DHCP options.
cable helper-address	Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or subinterface.
ip dhcp ping packet 0	Instructs the DHCP server to assign an IP address from its pool without first sending an ICMP ping to test whether a client is already currently using that IP address.

Command	Description
ip dhcp relay information option	Configures the DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp smart-relay	Enables the DHCP relay agent on the CMTS to automatically switch a cable modem or CPE device to a secondary DHCP server or address pool if the primary DHCP server does not respond to three successive requests.