



Cable Commands: q through sg

Revised: November 13, 2009, OL-15510-10

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

Modified Commands

Command	Cisco IOS Software Release
redundancy force-switchover	12.2(33)SCA
service class	12.2(33)SCA

Command	Cisco IOS Software Release
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

Removed Commands

Command	Cisco IOS Software Release
service divert-rate-limit	12.2(33)SCB

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		
	<i>profile-id</i>	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 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 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

<i>rcp-id</i>	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	
<i>index</i>	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.
<i>Hz</i>	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.
<i>index</i>	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)# rcc-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.
rcc-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

<i>index</i>	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.
<i>Hz</i>	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.
<i>index</i>	(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

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description This command has no arguments or keywords.

Command Default No default behaviors or values.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
	12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
	12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
	12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
	12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
	12.2(20)S	This command was implemented on the Cisco 7304 router.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
	12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
	12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
	12.3(11)T	This command was implemented on the MWR 1900 MWR.
	12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
	12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
	12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, INternetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Examples

The following example enables redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example assigns the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example configures two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-red)# linecard-group 1 y-cable
Router(config-red-lc)# member subslot 2/1 primary
Router(config-red-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# config t
```

```
Router(config)# redundancy
Router(config-r)# ?
```

```
Redundancy configuration commands:
  associate Associate redundant slots
  exit      Exit from redundancy configuration mode
  main-cpu  Enter main-cpu mode
  no       Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers.

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

To force the standby Route Processor (RP) to assume the role of the active RP, use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover [main-cpu]

Syntax Description	main-cpu	(Optional) Forces switchover to the main CPU.
---------------------------	-----------------	-----------------------------------------------

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.0(16)ST	This command was introduced.
	12.1(10)EX2	This command was integrated into Cisco IOS Release 12.1(10)EX2.
	12.0(17)ST	This command was implemented on the Cisco 12000 series routers.
	12.0(22)S	This command replaces the force-failover command on the Cisco 10000 series routers.
	12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
	12.2(18)S	This command was implemented on the Cisco 7500 series routers.
	12.2(20)S	Support was added for the Cisco 7304 router.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines	Use the redundancy force-switchover command to switch control of a router from the active RP to the standby RP. Both the active and standby RPs must have a high availability Cisco IOS image installed and must be configured for Route Processor Redundancy (RPR) mode before the redundancy force-switchover command can be used. Before the system switches over, it verifies that the standby RP is ready to take over.
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

When you use the **redundancy force-switchover** command and the current running configuration is different from the startup configuration, the system prompts you to save the running configuration before the switchover is performed.

**Note**

Before using this command in Cisco 7600 series routers, refer to the “Performing a Fast Software Upgrade” section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* for additional information.

On Cisco 7600 series routers, the **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The active and redundant supervisor engines do not reset on a Route Processor Redundancy Plus (RPR+) switchover. The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

Beginning with Cisco IOS Release 12.2(33)SCA, you can force a Performance Routing Engine (PRE) switchover using the **redundancy force-switchover main-cpu** command from either the primary or standby PRE. If you force a switchover from the active PRE, both PREs synchronize and the active PRE reloads normally. When you force a switchover from the standby PRE, a crash dump of the active PRE occurs for troubleshooting purposes. Forcing a switchover from the standby PRE should only be done if you cannot access the active PRE.

Examples

The following example shows a switchover from the active RP to the standby RP on a Cisco 7513 router with RPR configured:

```
Router# configure terminal
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# slave auto-sync config
Router(config)# redundancy
Router(config-r)# mode rpr
Router(config-r)# end
Router# copy running-config startup-config
Router# redundancy force-switchover
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover

System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y

00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover

Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Related Commands	Command	Description
	clear redundancy history	Clears the redundancy event history log.
	hw-module sec-cpu reset	Resets and reloads the standby RP with the specified Cisco IOS image and executes the image.
	hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RP.
	mode (HSA redundancy)	Configures the High System Availability (HSA) redundancy mode.
	mode (redundancy)	Configures the redundancy mode of operation.
	redundancy	Enters redundancy configuration mode.
	show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

redundancy reload

To reset the standby PRE module or to reset both the active and standby PRE modules, use the **redundancy reload** command in privileged EXEC mode.

redundancy reload {peer | shelf}

Syntax Description

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

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.

Usage Guidelines

The **redundancy reload peer** command reloads the Cisco IOS software on the standby PRE1 module, which does not have an impact on router 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 PRE1 modules, which will interrupt services on the router until all PRE1 modules and line cards initialize and come back online.

Examples

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

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



Note

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

The following example shows the system's response when a standby PRE1 module is not installed in the 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 both PRE1 modules:

```
Router# 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 modules. Pressing any other key aborts the reload and returns control to the current active PRE1 module.

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 PRE module becomes the active PRE module.
redundancy switch-activity	Forces a switchover to the standby PRE 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

<i>profile-id</i>	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	<i>time</i>	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

<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA FPGA. Valid values for <i>rf-port</i> depend on the configuration set with the annex modulation command.
<i>channel-id</i>	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		
<i>rf-channel</i>	RF channel physical port on the Wideband SPA. The allowed range is from 0 to 3.	
<i>depi-tunnel-name</i>	Name of the DEPI tunnel.	
tsid <i>id</i>	(Optional) 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:

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

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

<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for <i>rf-port</i> 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
```

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 SPA, 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		
<i>rf-port</i>		Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for <i>rf-port</i> depend on the configuration set with the annex modulation command (see the Usage Guidelines section).
<i>freq</i>		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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. The default value for interleave-depth is 32.

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: <ul style="list-style-type: none"> • 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.

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		
<i>rf-port</i>		Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 23. Valid values for <i>rf-port</i> depend on the configuration set with the annex modulation command (see the Usage Guidelines section).
<i>ip-address</i>		Specifies the IP address of the Gigabit Ethernet interface on the edge QAM device for this RF channel.
<i>mac-address</i>		Specifies the MAC address of the next-hop interface or of the edge QAM device for this RF channel.
<i>portnum</i>		Specifies the UDP port number for the edge QAM device that will be used for this RF channel. Allowed range is 0 to 65535.
<i>session-id</i>		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 to 18 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
```

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

```
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

<i>rf-port</i>	RF channel physical port on the Wideband SPA FPGA. The allowed range is from 0 to 23. The valid values for <i>rf-port</i> depend on the configuration set with the annex modulation command (see the Usage Guidelines section).
<i>delay</i>	Converged Interconnect Network (CIN) delay. The default value is 550 us. The allowed range is from 0 to 3000 us. The <i>delay</i> 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 <i>delay</i> value is set to auto.
<i>rate</i>	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 to 18 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 the Cisco UBR-MC20X20V cable interface line card, use the **rf-channel rf-power** command in controller integrated-cable or controller modular-cable 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		
	<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 3. Valid values for <i>rf-port</i> depend on the configuration set with the annex modulation command (see the Usage Guidelines section).
	<i>power-level</i>	Desired RF output power level in dBmV.

Command Default See Usage Guidelines.

Command Modes Controller configuration (config-controller)

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

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.



Note The RF power level can be configured in decimals too.

Following are the recommended RF power range for different channel settings.

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 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

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 SPA, use the **rf-channel rf-shutdown** command in controller integrated-cable or controller modular-cable 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

<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA FPGA. Allowed range is 0 to 3. Valid values for <i>rf-port</i> 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

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 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.
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.

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	Forces a manual switchover between the active and standby PRE1 modules.
	main-cpu	

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.
	<i>service-class-name</i>	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
```

Syntax Description

enforced	Specifies an enforced service class.
registered	Specifies enforcing of QoS profiles for the registered service class.
<i>name</i>	Specifies the name of the service class.

Command Default

No default behavior or values

Command Modes

Enforce-rule configuration (enforce-rule)

Command History

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

Usage Guidelines

The **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
```

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.
enabled (enforce-rule)	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.

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 interface 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

<i>divert-code rate</i>	Configures the PXF Divert-Rate-Limit for the any of the following packets: <ul style="list-style-type: none"> • fwd-glean—Packets that hit a glean adjacency in the FIB. • rpf-glean—Packets that hit a glean adjacency during the RPF check. <p>The minimum rate is 1 packet-per-second and the maximum rate is 255 packets-per-second.</p> <p>The default rate is 20 packets-per-second.</p>
limit <i>limit</i>	(Optional) Sets the limit for the number of packets that will be diverted in an initial burst of packets.
	The minimum limit is 4 packets and the maximum limit is 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

Interface configuration—cable interface only (config-if)

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-if)# 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-if)# 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
  vcci undefined          packets          bytes
  vcci C                  0               0
  ...
  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 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		
<i>ip-address</i>		Specifies the source IP address that should be matched. Example: 64.12.13.0
mask <i>ip-address</i>		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 <i>tos-value</i>		The ToS value of the trusted site. There are no restrictions on the <i>tos_value</i> . Example: 0xD0
mask <i>tos-mask</i>		The mask to apply to the IP ToS value and the trusted-site <i>tos_value</i> before testing if it matches. There are no restrictions on the <i>tos_mask</i> value. Example: 0xF3
		
	Note	The ToS value can be wild-carded by setting the <i>tos_mask</i> to 0x00
vrf <i>vrf-name</i>		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 <i>tos-mask</i> . 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 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		
	<i>divert-code</i>	Specifies the applicable divert code.
	<i>rate</i>	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.
	<i>limit</i>	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		
<i>ip-address</i>	Specifies the source IP address that should be matched. Example: 64.12.13.0	
mask <i>ip-address</i>	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 <i>tos-value</i>	The ToS value of the trusted site. There are no restrictions on the <i>tos_value</i> . Example: 0xD0	
mask <i>tos-mask</i>	The mask to apply to the IP ToS value and the trusted-site <i>tos_value</i> before testing if it matches. There are no restrictions on the <i>tos_mask</i> value. Example: 0xF3	
		
	Note	The ToS value can be wild-carded by setting the <i>tos_mask</i> to 0x00
vrf <i>vrf-name</i>	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 <i>tos-mask</i> . 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. 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.

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 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	<i>id</i>	Service instance ID.
	<i>service-type</i>	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*

Related Commands	Command	Description
	cable dhcp-giaddr policy	Sets the DHCP <i>giaddr</i> 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		
	<i>class</i>	Specifies service class number. Valid range is 1 to 16. Default value is 1.
	guaranteed-upstream <i>us-bandwidth</i>	Specifies the guaranteed upstream bandwidth in kbps. Valid range for <i>us-bandwidth</i> is 0 to 100000 kbps. Default value is 0.
	max-burst <i>burst-size</i>	Specifies the maximum upstream burst size in bytes. Valid range for <i>burst-size</i> 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 <i>max-dsbandwidth</i>	Specifies the downstream bandwidth in kbps. Valid range for <i>max-dsbandwidth</i> is 0 to 100000 kbps. Default value is 0.
	max-upstream <i>max-usbandwidth</i>	Specifies the upstream bandwidth in kbps. Valid range for <i>max-usbandwidth</i> is 0 to 100000 kbps. Default value is 0.
	priority <i>priority-num</i>	Specifies the service class priority. Valid range for <i>priority-num</i> 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	<i>string</i>	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.
	<i>service-type-id</i>	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

<i>ip-address</i>	Specifies the IP address of the multicast QoS group.
<i>ip-mask</i>	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

<i>time-date</i>	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 <i>giaddr</i> 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.

