Cable Commands: i through p

Revised: August 12, 2013, OL-15510-17

New Commands

Command	Cisco IOS Software Release
packetcable gate send-subscriberID	12.3(23)BC1
ipdr associate	12.2(33)SCB
ipdr collector	12.2(33)SCB
ipdr explorer start	12.2(33)SCB
ipdr session	12.2(33)SCB
ipdr session (global configuration)	12.2(33)SCB
ipdr template	12.2(33)SCB
issu linecard abortversion	12.2(33)SCB
issu linecard acceptversion	12.2(33)SCB
issu linecard changeversion	12.2(33)SCB
issu linecard loadversion	12.2(33)SCB
issu linecard prepareversion	12.2(33)SCB
issu linecard reloadversion	12.2(33)SCB
issu linecard runversion	12.2(33)SCB
match-rule	12.2(33)SCB
init-tech-list	12.2(33)SCC
init-tech-ovr	12.2(33)SCC
interface integrated-cable	12.2(33)SCC
interval	12.2(33)SCC
logging cmts sea	12.2(33)SCC
method	12.2(33)SCC
name	12.2(33)SCC
oui	12.2(33)SCC
output-rate	12.2(33)SCC

Command	Cisco IOS Software Release
override	12.2(33)SCC
policy	12.2(33)SCC
ipdr type	12.2(33)SCD2
prefix	12.2(33)SCC
license feature evaluation disable	12.2(33)SCE
license feature evaluation enable	12.2(33)SCE
protect-tunnel	12.2(33)SCE
logging cmts ipc-cable	12.2(33)SCF
ipdr exporter ack-timeout	12.2(33)SCG
ipdr exporter keepalive	12.2(33)SCG
ipdr exporter max-unacked	12.2(33)SCG
periodic-rel-pxf_enable	12.2(33)SCG2

Modified Commands

Command	Cisco IOS Software Release
member subslot	12.2(33)SCA
mode (redundancy)	12.2(33)SCA
ping docsis	12.2(33)SCA
interface cable	12.2(33)SCA
interface modular-cable	12.2(33)SCB
interface wideband-cable	12.2(33)SCB
ip accounting mac-address	12.2(33)SCB
mac-address	12.2(33)SCB
mtu	12.2(33)SCB
negotiation	12.2(33)SCB
packetcable gate send-subscriberID	12.2(33)SCB
penalty-period	12.2(33)SCB
plim qos input map	12.2(33)SCB
ping docsis	12.2(33)SCC
interface cable	12.2(33)SCD
interface wideband-cable	12.2(33)SCD
peak-time1	12.2(33)SCD2
penalty-period	12.2(33)SCD2
member subslot	12.2(33)SCC4
interface cable	12.2(33)SCE
interface modular-cable	12.2(33)SCE

Command	Cisco IOS Software Release
interface Wideband-Cable	12.2(33)SCE
mode (redundancy)	12.2(33)SCE
interval	12.2(33)SCE1
ipdr template	12.2(33)SCG

init-tech-list

To set the DCC initialization techniques that the CMTS can use to load balancing cable modems, use the **init-tech-list** command in the config-lb-group configuration mode. To reset the DCC initialization techniques, use the **no** form of this command.

init-tech-list *grouplist* [**ucc**]

no init-tech-list

Syntax Description

grouplist	DCC initialization technique list.
ucc	(Optional) Determines whether Upstream Channel Change (UCC) can be used for modems during dynamic upstream load balancing.

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.

Examples

The following example shows how to set the DCC initialization techniques on a DOCSIS load balancing group on the CMTS, using the **init-tech-list** 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)# init-tech-list 1 ucc
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.

init-tech-ovr

To set DCC initialization techniques that override the physical upstream channel pair, use the **init-tech-ovr** command in the config-lb-group configuration mode.

Cisco uBR10012 Router

init-tech-ovr cable *slot/subslot/port upstream* **cable** *slot/subslot/port upstream* **init-tech-list** *0-4* **[ucc]**

Cisco uBR7225VXR and Cisco uBR7246VXR Routers

init-tech-ovr cable *slot/port upstream* **cable** *slot/port upstream* **init-tech-list** *0-4* **[ucc]**

Syntax Description

cable *slot/subslot/port upstream*	Specifies the CMTS interface slot, subslot, port number, and upstream parameters that are to be overridden. • *slot*—Slot where the line card resides. Ther permitted range is from 5 to 8. • *subslot*—Subslot where the line card resides. The available slots are 0 or 1. • *port*—The downstream controller number on the line card. The permitted *port* range is from 0 to 4.
cable *slot/subslot/port upstream*	Specifies the CMTS interface slot, subslot, port number, and upstream channel ID parameters that will override the CMTS interface and upstream channel.
cable *slot/port upstream*	Specifies the CMTS interface slot, port number, and upstream parameters that are to be overridden. • *slot*—Slot where the line card resides. – Cisco uBR7225VXR router—The valid range is from 1 to 2. – Cisco uBR7246VXR router—The valid range is from 3 to 6. • *port*—Downstream controller number on the line card. The permitted *port* values are 0 or 1.
cable *slot/port upstream*	Specifies the CMTS interface slot, port number, and upstream parameters that will override the CMTS interface and upstream channel.
init-tech-list *0-4*	Specifies the DCC initialization technique list ranging from 0 to 4 for the upstream channel pair.
ucc	Determines whether Upstream Channel Change (UCC) can be used for modems during dynamic upstream load balancing.

Command Default

None

Command Modes

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

Command History

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

Usage Guidelines

The **init-tech-list** command accepts an upstream that is not added into the load balancing group. The upstream channel pair is invalid until the upstream is added. When the load balancing group is removed, all upstream channel pairs are also removed.

Examples

The following example shows how to set DCC initialization techniques that override the physical upstream channel pair to a DOCSIS load balancing group on the CMTS, using the **init-tech-ovr** 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)# init-tech-ovr cable 1/0 1 cable 1/1 2 1
```

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.

interface cable

To configure a cable interface, use the **interface cable** command in global configuration mode.

interface cable {*slot*/*port* | *slot*/*subslot*/*port*}

Cisco IOS Release 12.2(33)SCE and later

interface cable {*slot*/*cable-interface-index* | *slot*/*subslot*/*cable-interface-index*}

Syntax Description

slot	Slot where the line card resides. • Cisco uBR7225VXR router—The valid value is 1 or 2. • Cisco uBR7246VXR router—The valid range is from 3 to 6. • Cisco uBR10012 router—The valid range is from 5 to 8.
subslot	(Cisco uBR10012 only) Secondary slot number of the cable interface line card. The valid subslots are 0 or 1.
port	Downstream port number. • Cisco uBR7225VXR router and Cisco uBR7246VXR router—The valid value is 0 or 1. • Cisco uBR10012 router—The valid range is from 0 to 4 (depending on the cable interface).
cable-interface-index	Downstream port of the Cisco uBR10-MC5X20 and Cisco uBR-MC28 line cards, or MAC domain index of the Cisco uBR-MC20X20V and Cisco uBR-MC3GX60V line cards. Cisco uBR7225VXR and Cisco uBR7246VXR routers—The valid port value is 0 or 1. Cisco uBR10012 router—The valid range for the Cisco uBR-MC20X20V and Cisco uBR-MC5X20 line cards is from 0 to 4. The valid range for the Cisco uBR-MC3GX60V line card is from 0 to 14.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced.
12.3(23)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Release	Modification
12.2(33)SCD	This command was modified to support Cisco uBR7225VXR and Cisco uBR7246VXR routers.
12.2(33)SCE	This command was modified. The *port* parameter was changed to *cable-interface-index* to indicate the MAC domain index for the Cisco uBR-MC20X20V and Cisco uBR-MC3GX60V cable interface line cards.

Examples

The following example shows how to configure a cable interface in slot 5, and port 0 on a Cisco uBR7246VXR or Cisco uBR7225VXR router:

```
Router# configure terminal
Router(config)# interface cable 5/0
```

The following example shows how to configure a cable interface in slot 8, subslot 0, and port 0 on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 8/0/0
```

The following example shows how to configure a Cisco uBR-MC3GX60V cable interface line card in slot 5, subslot 0, and cable interface index 13 (MAC domain index) on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 5/0/13
```

Related Commands

Command	Description
interface integrated-cable	Specifies a integrated cable interface.
interface modular-cable	Specifies a modular cable interface.
interface wideband-cable	Specifies a wideband cable interface.

interface cable-modem

To enter interface configuration mode for the cable interface on a router, use the **interface cable-modem** command in global configuration mode.

Cisco uBR904, uBR905, uBR924, uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

interface cable-modem *number*

Syntax Description

number	Identifies the cable interface (always **0**).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)NA	This command was introduced for the Cisco uBR904 cable access router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.

Usage Guidelines

When this command is entered, the router switches from global configuration mode to interface configuration mode.

Examples

The following example shows how to enter interface configuration mode for the router's cable interface and then to enter the available interface configuration commands:

```
Router(config)# interface cable-modem 0
Router(config-if)# cable-modem ?
  compliant    Enter compliant modes for interface
  downstream   Downstream channel characteristics
  fast-search  Enable/disable the DS fast search
  upstream     upstream channel characteristics
  voip         Options for Voice over IP traffic over the cable interface

Router(config-if)#
```

Related Commands

Command	Description
cable-modem compliant bridge	Enables DOCSIS-compliant bridging on the cable interface.
cable-modem downstream saved channel	Modifies the saved downstream channel setting and upstream power value on the cable interface.

cable-modem upstream preamble qpsk	Enables the QPSK modulation scheme in the upstream direction from the cable interface to the CMTS.
cable-modem voip best-effort	Allows voice traffic to be transmitted on the upstream using a best-effort QoS.

interface gigabitethernet

The **interface gigabitethernet** command is now documented as the **gigabitethernet** keyword of the **interface** command. For more information, see the **interface** command.

interface integrated-cable

To configure integrated cable interface, use the **interface integrated-cable** command in global configuration mode.

Cisco uBR10012 Universal Broadband Router

interface integrated-cable *slot/subslot/port:rf-channel*

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Router

interface integrated-cable *slot/port:rf-channel*

Syntax Description

slot	Identifies the chassis slot where the cable interface line card resides. • Cisco uBR10012 router—The valid range is from 5 to 8. • Cisco uBR7225VXR router—The valid value is 1 or 2. • Cisco uBR7246VXR router—The valid range is from 3 to 6.
subslot	(Cisco uBR10012 only) Secondary slot number of the cable interface line card. The valid subslots are 0 or 1.
port	Downstream port number. • Cisco uBR7225VXR router and Cisco uBR7246VXR router—The valid value is 0 or 1. • Cisco uBR10012 router—The valid range is from 0 to 4.
rf-channel	RF channel number. The valid range is from 0 to 3.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **interface integrated-cable** command is supported only on Cisco uBR-MC88V and Cisco UBR-MC20X20V line cards.

Examples

The following example shows how to configure a integrated cable interface in slot 7, subslot 0, and port 0 on a Cisco UBR-MC20X20V cable interface line card:

```
Router# configure terminal
Router(config)# interface integrated-cable 7/0/0:1
```

Associated Features

The **interface integrated-cable** command is used to configure the following:

- Configuring the Cisco UBR-MC20X20V Cable Interface Line Card
- Configuring the Cisco uBR-MC88V Cable Interface Line Card

Related Commands

Command	Description
show interface integrated-cable	Displays the current configuration and status for an integrated channel.

interface modular-cable

To configure a modular cable interface, use the **interface modular-cable** command in global configuration mode.

Cisco IOS Releases 2.3(21)BC, 12.3(23)BC, and 12.2(33)SCA

interface modular-cable *slot*/*subslot*/*bay*:*nb-channel-number*

Cisco IOS Release 12.2(33)SCB

interface modular-cable *slot*/*bay*/*port*:*nb-channel-number*

Cisco IOS Release 12.2(33)SCE

interface modular-cable *slot*/{*subslot* | *bay*}/*port*:*interface-number*

Syntax Description

slot	Identifies the chassis slot where the Cisco Cable line card, or Cisco Wideband Shared Port Adaptor (SPA) is located. • For the Cisco Cable line cards, the valid range is from 5 to 8. • For the Cisco Wideband SPA, the valid values are: – *slot*—1 or 3 (for SIP-600) – *slot*—1 (for Wideband SIP) **Note** In Cisco IOS Release 12.2(33)SCE, support for configuring modular-cable interface on the Cisco uBR-MC3GX60V cable line card is introduced.
subslot	Identifies the subslot where the Cisco Cable line card is located. • For the Cisco Cable line cards, the valid value is 0 or 1. **Note** In Cisco IOS Release 12.2(33)SCE, support for configuring modular-cable interface on the Cisco uBR-MC3GX60V cable line card is introduced.
bay	Identifies the bay where the Cisco Wideband SPA is located. The valid range is from 0 to 3.
port	Identifies the port on the Cisco Cable line card, or the Cisco Wideband SPA in the specified *slot*/*subslot* or *slot*/*bay*. • For the Cisco UBR-MC20X20V cable interface line card, the valid range for is from 0 to 5. • For the Cisco uBR-MC3GX60V cable interface line card, the valid range is from 0 to 2. • For the Cisco Wideband SPA, the valid value is 0.
nb-channel-number	Identifies the narrowband channel number.
interface-number	Identifies the modular-cable interface number. The valid range is from 0 to 23.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced.
12.3(23)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCB	This command was modified to change the addressing format for the modular cable interface from *slot/subslot/bay:nb-channel-number* to *slot/bay/port:nb-channel-number*.
12.2(33)SCE	Support for configuring modular-cable interface on the Cisco uBR-MC3GX60V cable line card was introduced.

Examples The following example shows how to configure a modular cable interface in slot 1, bay 3, and channel 23 on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface modular-cable 1/3/0:23
```

The following example shows how to configure a modular cable interface in slot 5, subslot 1, and port 2 on a Cisco uBR-MC3GX60V cable line card.

```
Router# configure terminal
Router(config)# interface modular-cable 5/1/2:0
```

Related Commands

Command	Description
cable attribute-mask	Specifies an attribute mask value for a modular cable interface.
interface wideband-cable	Specifies a wideband cable interface.
interface cable	Specifies a cable interface.

interface port-channel

To create an EtherChannel interface on the Cisco Cable Modem Termination System (CMTS), use the **interface port-channel** command in global configuration mode. To remove this EtherChannel port from the Cisco CMTS, use the **no** form of this command.

interface port-channel *n*

no interface port-channel *n*

Syntax Description

number	Identifying port channel number for this interface (EtherChannel port). The range is 1 to 64.

Command Default

By default, EtherChannel groups and ports are not defined, and they are disabled (**off** mode) configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)BC3	This command was introduced on the Cisco uBR7246VXR router.
12.2(9a)BC	This command was introduced on the Cisco uBR10012 router.

Usage Guidelines

The first EtherChannel interface configured becomes the bundle master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is later removed, the second EtherChannel interface to be configured becomes the bundled master by default.

Repeat this configuration on every EtherChannel port to be bundled into a FastEtherChannel (FEC) or GigabitEtherChannel (GEC) group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.

For additional information about using the EtherChannel feature on the Cisco CMTS, refer to the following document on Cisco.com:

- *EtherChannel for the Cisco CMTS*

Examples

The following example configures the port to have an EtherChannel port number of 1 within its EtherChannel group. The EtherChannel group is defined with the **channel-group** command.

```
Router(config-if)# interface port-channel 1
```

Related Commands

Command	Description
channel-group	Assigns an EtherChannel port to an EtherChannel group.
show interface port-channel	Displays the EtherChannel interfaces and channel identifiers, with their mode and operational status.

interface usb

To enter the interface configuration mode for the Universal Serial Bus (USB) interface, use the **interface usb** command in global configuration mode.

Cisco uBR925 cable access router, Cisco CVA122 Cable Voice Adapter

interface usb *number*

Syntax Description

number	Identifies the USB interface (always **0**).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(5) XU1	This command was introduced for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.

Usage Guidelines

When this command is entered, the router switches from global configuration mode to interface configuration mode for the USB interface.

Examples

The following example shows how to enter interface configuration mode for the USB interface and then to display the available commands:

```
Router(config)# interface usb 0
Router(config-if)#?
Interface configuration commands:
  access-expression       Build a bridge boolean access expression
  arp                     Set arp type (arpa, probe, snap) or timeout
  bandwidth               Set bandwidth informational parameter
  bridge-group            Transparent bridging interface parameters
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  crypto                  Encryption/Decryption commands
  custom-queue-list       Assign a custom queue list to an interface
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  exit                    Exit from interface configuration mode
  fair-queue              Enable Fair Queuing on an Interface
  h323-gateway            Configure H323 Gateway
  help                    Description of the interactive help system
  hold-queue              Set hold queue depth
  ip                      Interface Internet Protocol config commands
  keepalive               Enable keepalive
```

```
  load-interval           Specify interval for load calculation for an
                          interface
  logging                 Configure logging for interface
  mac-address             Manually set interface MAC address
  max-reserved-bandwidth  Maximum Reservable Bandwidth on an Interface
  mtu                     Set the interface Maximum Transmission Unit (MTU)
  no                      Negate a command or set its defaults
  ntp                     Configure NTP
  priority-group          Assign a priority group to an interface
  random-detect           Enable Weighted Random Early Detection (WRED) on an
                          Interface
  service-policy          Configure QoS Service Policy
  shutdown                Shutdown the selected interface
  snmp                    Modify SNMP interface parameters
  standby                 Interface HSRP configuration commands
  timeout                 Define timeout values for this interface
  traffic-shape           Enable Traffic Shaping on an Interface or
                          Sub-Interface
  transmit-interface      Assign a transmit interface to a receive-only
                          interface
  tx-ring-limit           Configure PA level transmit ring limit

Router(config-if)#
```

Related Commands

Command	Description
show controllers usb	Displays the high-level controller information for the USB interface.
show interfaces usb	Displays configuration information about the USB interface.

interface wideband-cable

To configure a wideband cable interface, use the **interface wideband-cable** command in global configuration mode.

Cisco uBR10012 Universal Broadband Router

Cisco IOS Releases 12.3(21)BC, 12.3(23)BC, and 12.2(33)SCA

interface wideband-cable *slot/subslot/bay*:*wideband-channel*

Cisco IOS Release 12.2(33)SCB

interface wideband-cable *slot/bay/port*:*wideband-channel*

Cisco IOS Release 12.2(33)SCC

interface wideband-cable *slot/*{*subslot* | *bay*}*/port*:*wideband-channel*

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers

Cisco IOS Release 12.2(33)SCD

interface wideband-cable *slot/port*:*wideband-channel*

Syntax Description

slot	The slot where a SIP or cable line card resides. • Cisco uBR7246VXR router—The valid range is from 3 to 6. • Cisco uBR7225VXR router—The valid range is from 1 to 2. • Cisco uBR10012 router—The valid range for: – Cable line card is from 5 to 8 – SIP is 1 and 3
subslot	The subslot where a SIP or cable line card resides. • Cisco uBR10012 router—The valid value for: – Cable line card in slot 5 to 8 is 0 or 1 – SPAs in a SIP in slot 1 or 3, prior to Cisco IOS Release 12.2(33)SCB is 0 or 1. For Cisco IOS Release 12.2(33)SCB and later, subslot is not specified.
bay	The bay in a SIP where a SPA is located. The valid range is from 0 to 3.

port	Specifies the port number. • Cisco uBR7246VXR router and Cisco uBR7225VXR router—The valid range is from 0 to 1. • Cisco uBR10012 router—The valid value for: – Slot 1 and 3 is 0 – Slot 5 to 8 is from 0 to 4
wideband-channel	Represents the wideband channel number. • Cisco uBR10012 router—The valid range for: – Cisco UBR-MC20X20V cable interface line card is from 0 to 5. – Cisco uBR-MC3GX60V cable interface line card and SPAs is from 0 to 31. • Cisco uBR7246VXR and Cisco uBR7225VXR routers—The valid range is from 0 to 5.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced.
12.3(23)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCB	This command was modified to change the addressing format for the wideband cable interface from *slot/subslot/bay:wideband-channel* to *slot/bay/port:wideband-channel.*
12.2(33)SCD	This command was modified. Support was added for Cisco uBR7225VXR and Cisco uBR7246VXR routers.
12.2(33)SCE	Support was added for Cisco uBR-MC3GX60V cable interface line card on the Cisco uBR10012 router.

Examples

The following example shows how to configure a wideband cable interface in slot 1, bay 3, and port 0 on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface wideband-cable 1/3/0:0
```

The following example shows how to configure a wideband cable interface in slot 5, subslot 1, and port 2 on a Cisco uBR-MC3GX60V cable line card.

```
Router# configure terminal
Router(config)# interface wideband-cable 5/1/2:0
```

The following example shows how to configure a wideband cable interface in slot 1, and port 0 on a Cisco uBR7225VXR or Cisco uBR7246VXR router:

```
Router# configure terminal
Router(config)# interface wideband-cable 1/0:0
```

Related Commands

Command	Description
cable downstream attribute-mask	Specifies an attribute mask value for a wideband cable interface.
interface modular-cable	Specifies a modular cable interface.
interface cable	Specifies a cable interface.

interval

To set the duration of time the CMTS waits before checking the load on an interface, use the **interval** command in the load balancing group configuration mode. To reset the duration of time, use the **no** form of this command.

interval *seconds*

no interval

Syntax Description

seconds	The polling interval for the CMTS to determine the current load on each cable interface. The valid range is from 1 to 1000. The default value is 10 seconds in Cisco IOS Release 12.2(33)SCE and earlier. The default value is 30 seconds in Cisco IOS Release 12.2(33)SCE1 and later.

Command Default

None

Command Modes

Load balancing group configuration (config-lb-group)

Command History

Release	Modification
12.2(33)SCC	This command was introduced.
12.2(33)SCE1	This command was modified. The default value for this command was changed from 10 seconds to 30 seconds.

Examples

The following example shows how to set the duration of time that the CMTS waits before checking the load on the interface, using the **interval** 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)# interval 50
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.

ip-address (controller)

To set the IP address of the Wideband SPA FPGA, use the **ip-address (controller)** command in controller configuration mode. To remove the IP address of the Wideband SPA FPGA, use the **no** form of this command.

ip-address *ip-address*

no ip-address *ip-address*

Syntax Description

ip-address	IP address for the Wideband SPA FPGA.

Command Default

No IP address is set for the Wideband SPA FPGA.

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

Use this command to set the IP address for the Wideband SPA FPGA. This address is used as the source IP address for packets that the Wideband SPA transmits to the EQAM device.

Examples

The following example shows how to set the IP address of the Wideband SPA FPGA. The SPA is located in slot 1, subslot 0, bay 0.

```
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# ip-address 192.168.200.6
```

Related Commands

Command	Description
annex modulation	Sets the annex and modulation for the Wideband SPA.
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.
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.

Command	Description
rf-channel description	Specifies the description for each RF channel.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.

ip address docsis

To specify that the cable access router should use the DHCP protocol, as required by the DOCSIS specification, to assign an IP address for its cable interface, use the **ip address docsis** command in cable interface configuration mode. To disable the use of DHCP, use the **no** form of this command.

Cisco uBR905, uBR924, uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

ip address docsis

no ip address docsis

Syntax Description

There are no key words or arguments for this command.

Command Default

The cable access router uses the DHCP protocol, as required by the DOCSIS specification, to assign an IP address to its cable interface during system power-on.

Command Modes

Interface configuration (cable interface only)

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.1(4)T	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.

Usage Guidelines

The **ip address docsis** command configures the cable access router so that it obtains its IP address from a DHCP server at system power-on, which is a requirement for DOCSIS operation. This is the default mode of operation. If the configuration for the cable interface does not include any form of **ip address** command, the cable access router defaults to configuring the cable interface with the **ip address docsis** command.

Configuring the cable interface with any other form of the **ip address** command or with the **no ip address docsis** command prevents the cable access router from operating in DOCSIS networks. This mode of operation should be used only in lab or test networks.

Note Earlier Cisco IOS software releases for the cable access routers used either the **ip address negotiated** or the **ip address dhcp** command to specify that the cable interface should obtain its IP address from a DHCP server. These commands should no longer be used to configure the router's cable interface.

Examples

The following example shows how to configure the cable access router so that it obtains the IP address for its cable interface from a DHCP server:

```
Router(config)# interface cable-modem 0
Router(config-if)# ip address docsis
Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
cable-modem dhcp-proxy	Specifies that a DHCP server should provide the IP address for the router's Ethernet interface or for a NAT address pool.
ip http dhcp	Specifies the use of the DHCP protocol to obtain an IP address for any interface except the cable interface at system power-on.
ip http negotiated	Specifies that a serial interface should use the PPP/IPCP to obtain an IP address at system power-on

ip http cable-monitor

To enable the cable access router's onboard Cable Monitor web server, use the **ip http cable-monitor** command in global configuration mode. To disable the Cable Monitor and turn off all access to the onboard Cisco web server, use the **no** form of this command.

Cisco uBR905, uBR924, uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

ip http cable-monitor {**basic** | **advance**} [*url-ip-address url-mask*]

no ip http cable-monitor

Syntax Description

basic	Displays only the basic status and performance pages.
advance	Displays all status and diagnostic pages. **Note** The Cable Monitor should not be used in advanced mode without first implementing a secure password strategy on the cable access router. Enabling the Cable Monitor in advanced mode without setting an encrypted enabled password could provide information that would allow remote users to change the router's configuration.
url-ip-address	(Optional) Specifies the IP address for the Cable Monitor. This argument, along with the *url-mask* argument, also defines the network that provides the IP address pool used by the temporary DHCP server when the cable interface goes down.
url-mask	(Optional) Specifies the subnet mask for the Cable Monitor. This argument, along with the *url-ip-address* argument, also defines the network that provides the IP address pool used by the temporary DHCP server when the cable interface goes down.

Command Default

For *url-ip-address*, 192.168.100.1

For *url-mask*, 255.255.255.0

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command is introduced for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.

Usage Guidelines

This command enables the Cable Monitor, an onboard web server that displays current status, troubleshooting, and performance information. The Cable Monitor can be accessed in two ways:

- When the cable access router has established connectivity with the CMTS over the cable interface, a service technician can use a web browser to remotely access the router and display the desired information.
- When the cable network is not operational and the cable access router is not online, the subscriber can access the tool with a PC connected to the router's Ethernet ports. Technicians can then prompt the user for the information they need to determine the source of the problem.

Enabling the Cable Monitor also enables the Cisco web server that is onboard the cable access router, which is the equivalent to entering the **ip http server** command. However, when the Cable Monitor is enabled, all other access, including CLI access, to the onboard web server is automatically disabled.

Note When the Cable Monitor is enabled in the startup configuration file, the messages "Starting DNS process" and "Terminating DNS process" can appear in the messages displayed during boot-up on the console. These messages are normal and can be ignored.

Disabling the Cable Monitor using the **no ip http cable-monitor** command also automatically disables the Cisco web server, which is the equivalent of giving the **no ip http server** command. When disabling the Cable Monitor, the console might display warning messages similar to the following:

```
% monitor-209.165.202.131 is not in the database.
% monitor-192.168.100.1 is not in the database.
% Range [209.165.202.131, 209.165.202.131] is not in the database.
% Range [192.168.100.1, 192.168.100.1] is not in the database.
```

These messages can be ignored because they are simply confirming that the IP addresses used for the Cable Monitor are no longer being used for that purpose.

The *URL-IP-address* and *URL-mask* arguments also specify that the class C private network 192.168.100.0 is the default address pool for the temporary DHCP server that activates when the cable interface goes down.

Note The Cable Monitor web interface does not work with the Cisco Easy VPN Remote web interface. To access the Cable Monitor web interface, you must first disable the Cisco Easy VPN Remote web interface with the **no ip http ezvpn** command, and then enable the Cable Monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cable Monitor for advanced mode, in which all status and diagnostic pages are displayed:

```
Router(config)# ip http cable-monitor advance
Router(config)#
```

The following example shows how to disable both the Cable Monitor and the Cisco web server, preventing all web server access to the Cisco uBR924 cable access router:

```
Router(config)# no ip http cable-monitor
Router(config)#
```

Related Commands

Command	Description
ip http ezvpn	Enables the enable the Cisco Easy VPN Remote web server interface.
ip http port	Configures the TCP port number for the router's HTTP web server. The default is the well-known web server port of 80.
ip http server	Enables and disables the router's HTTP web server.

Note The **ip http** command also supports two options, **access-class** and **authentication**, that should not be used when the Cable Monitor is enabled.

ip http ezvpn

To enable the Cisco Easy VPN Remote web server interface, use the **ip http ezvpn** command in global configuration mode. To disable the Cisco Easy VPN Remote web interface, use the **no** form of this command.

Cisco uBR905 and BR925 cable access routers

ip http ezvpn

no ip http ezvpn

Syntax Description

This command has no keywords or arguments.

Command Default

The Cisco Easy VPN Remote web interface is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YJ, 12.2(15)T	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. This allows the user to perform these functions without having to use the Cisco command-line interface.

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the **ip http server** command. Then use the **ip http ezvpn** command to enable the Cisco Easy VPN Remote web server. You can then access the web server by entering the IP address for the router's Ethernet interface in your web browser.

Note The Cisco Easy VPN Remote web interface does not work with the Cable Monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the Cable Monitor web interface, you must first disable the Cisco Easy VPN Remote web interface with the **no ip http ezvpn** command, and then enable the Cable Monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cisco Easy VPN Remote web server interface:

```
Router# configure terminal
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
Router# copy running-config startup-config
```

Related Commands

Command	Description
clear crypto ipsec client ezvpn	Resets the Cisco Easy VPN Remote state machine and bring down the Cisco Easy VPN Remote connection.
crypto ipsec client ezvpn xauth	Responds to a pending VPN authorization request.
crypto ipsec client ezvpn (global configuration)	(Global configuration mode) Creates a Cisco Easy VPN Remote configuration.
crypto ipsec client ezvpn (interface configuration)	(Interface configuration mode) Assigns a Cisco Easy VPN Remote configuration to an interface.
crypto ipsec client ezvpn connect	Manually connects to a specified IPSec VPN tunnel.
ip http cable-monitor	Enables and disables the Cable Monitor web server feature.
ip http port	Configures the TCP port number for the router's HTTP web server. The default is the well-known web server port of 80.
ip http server	Enables and disables the router's HTTP web server.

ip-address (controller)

To set the IP address of the Wideband SPA FPGA, use the **ip-address (controller)** command in controller configuration mode. To remove the IP address of the Wideband SPA FPGA, use the **no** form of this command.

ip-address *ip-address*

no ip-address *ip-address*

Syntax Description

ip-address	IP address for the Wideband SPA FPGA.

Command Default

No IP address is set for the Wideband SPA FPGA.

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)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

Use this command to set the IP address for the Wideband SPA FPGA. This address is used as the source IP address for packets that the Wideband SPA transmits to the EQAM device.

Examples

The following example shows how to set the IP address of the Wideband SPA FPGA. The SPA is located in slot 1, subslot 0, bay 0.

```
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# ip-address 192.168.200.6
```

Related Commands

Command	Description
annex modulation	Sets the annex and modulation for the Wideband SPA.
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.
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.

Command	Description
rf-channel network delay	Specifies the CIN delay for each RF channel.
rf-channel description	Specifies the description for each RF channel.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.

ipdr associate

To associate the Collector with a session, use the **ipdr associate** command in global configuration mode. To remove the association, use the **no** form of this command.

ipdr associate *session_id collector_name priority*

no ipdr associate *session_id collector_name*

Syntax Description

session_id	The unique IPDR session ID.
collector_name	The collector name. The name should not contain extra spaces.
priority	The priority value between the session and the collector. The value range is 1 to 10. A value of 1 indicates that the highest priority.

Command Default

An association with the session will not be created.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command allows the user to associate the Collector with a session. Once the Collector is configured, the Exporter sends data to the Collector. IPDR supports redundant collector and consistent streaming continues when a collector is down or not functioning.

The **no** form of the command will only remove the association for the stopped session.

Note The collector and the session should be configured before running this command.

Examples

The following example configures a Collector.

```
Router# configure terminal
Router(config)#ipdr associate 1 federal 1
```

Related Commands

Command	Description
ipdr collector	Configures the IPDR Collector details.
show ipdr collector	Displays the collector information, message statistics and event for all the sessions that are associated with the collector.
ipdr session	Adds a session to the IPDR Exporter.

ipdr collector

To configure the Internet Protocol Detail Record (IPDR) Collector details, use the **ipdr collector** command in global configuration mode. To remove the Collector, use the **no** form of this command.

ipdr collector *collector_name ip_addr* [*port*]

no ipdr collector *collector_name*

Syntax Description

collector_name	The collector name. The name should not contain extra spaces.
ip_addr	The collector IP address.
port	(Optional) The collector port value. The default port number will be considered if the value is not entered.

Command Default

A Collector will not be configured.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command allows the user to configure an IPDR Collector and authenticate the IPDR protocol. Once the Collector is configured, the Exporter sends data to the Collector. User must provide the collector name and the IP address. Port number is used when an exporter creates an active connection.

The **no** form of the command will remove a specific IPDR Collector. If the collector is associated with an active session, you should stop the session before using the **no** command.

Examples

The following example configures a Collector.

```
Router# configure terminal
Router(config)#ipdr collector federal 192.0.2.0
```

Related Commands

Command	Description
show ipdr collector	Displays the collector information, message statistics and event for all the sessions that are associated with the collector.
ipdr session	Adds a session to the IPDR Exporter.

ipdr exporter ack-timeout

To set IPDR Exporter acknowledged records timeout value, use the **ipdr exporter ack-timeout** command in global configuration mode. To disable the acknowledged records timeout value, use the **no** form of this command.

ipdr exporter ack-timeout *time_interval*

no ipdr exporter ack-timeout

Syntax Description

time_interval	Acknowledged records timeout count. The valid range is from 5 to 60 seconds. The default value is 60.

Command Default

This command is enabled when the IPDR Exporter is running.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(33)SCG	This command was introduced.

Usage Guidelines

This command allows you to set acknowledged records timeout value for a session.

Note Restart the IPDR Exporter for the timer values to take effect.

Examples

The following example shows how to configure the acknowledged records timeout value on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ipdr exporter ack-timeout 60
Router(config)# ipdr exporter start
```

Related Commands

Command	Description
show ipdr exporter	Displays information about the IPDR Exporter state on the Cisco CMTS router.

ipdr exporter keepalive

To set the keepalive timer value on the IPDR exporter, use the **ipdr exporter keepalive** command in global configuration mode. To disable the keepalive timer value, use the **no** form of this command.

ipdr exporter keeepalive *time_interval*

no ipdr exporter keepalive

Syntax Description

time_interval	Keepalive timer count. The valid range is from 5 to 300 seconds. The default value is 300.

Command Default

This command is enabled when the IPDR Exporter is running.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(33)SCG	This command was introduced.

Usage Guidelines

This command allows you to set the keeplive timeout value for a session.

Note Restart the IPDR Exporter for the keepalive timer values to take effect.

Examples

The following example shows how to configure the keepalive value on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ipdr exporter keepalive 300
Router(config)# ipdr exporter start
```

Related Commands

Command	Description
show ipdr exporter	Displays information about the IPDR Exporter state on the Cisco CMTS.

ipdr exporter max-unacked

To set the maximum number of unacknowledged records on the IPDR exporter, on the Cisco CMTS, use the **ipdr exporter max unacked** command in global configuration mode. To reset the maximum number of unacknowledged records, use the **no** form of this command.

ipdr exporter max-unacked *records*

no ipdr exporter max-unacked

Syntax Description

records	Number of unacknowledged records. The valid range is from 5 to 200 records. The default value is 200.

Command Default

This command is enabled when IPDR Exporter is running.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(33)SCG	This command was introduced.

Usage Guidelines

This command allows you to set the maximum number of unacknowledged records for a session.

Note Restart the IPDR Exporter for the number of records to take effect.

Examples

The following example shows how to configure the number of unacknowledged records configured on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ipdr exporter max-unacked 200
Router(config)# ipdr exporter start
```

Related Commands

Command	Description
show ipdr exporter	Displays information about the IPDR Exporter state on the Cisco CMTS router.

ipdr exporter start

To enable the CMTS application, to start the Internet Protocol Detail Record (IPDR) Exporter process to connect the exporter and the collector, use the **ipdr exporter start** command in global configuration mode. To terminate the connection between the exporter and collector, use the **no** form of this command.

ipdr exporter start

no ipdr exporter start

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the IPDR exporter process will not be started.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command allows the user to explicitly start the IPDR Exporter and connect to the collector. As a default behavior, the command will initiate all the sessions configured in the Exporter to a "Start" state.

The **no** form of the command will stop the IPDR Exporter process. The command will also clear the connection with the collector while retaining other configurations.

Examples

The following example starts the IPDR Exporter process on the CMTS.

```
Router# configure terminal
Router(config)#ipdr exporter start
```

Related Commands

Command	Description
show ipdr exporter	Displays information about the IPDR Exporter state.
show ipdr collector	Displays the collector information, message statistics and event for all the sessions that are associated with the collector.
ipdr collector	Configures the Internet Protocol Detail Record (IPDR) Collector details.

ipdr session

To start or stop a specific session, use the **ipdr session** command in the privileged EXEC mode.

ipdr session *session_id* {**start** | **stop**}

Syntax Description

session_id	The unique IPDR session ID.
start	The keyword to start the session.
stop	The keyword to stop the session.

Command Default

No sessions are started.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to start or stop a specific session. This command can be executed only when the IPDR exporter is started.

Note The user has to stop the session before configuring any tasks if the session is active.

Examples

The following example enables the user to start a session.

```
Router# configure terminal
Router(config)#ipdr session 1 start
```

Related Commands

Command	Description
ipdr exporter start	Starts the IPDR Exporter and connects to the collector.
show ipdr exporter	Displays information about the IPDR Exporter state.
ipdr associate	Associates the Collector with a session.

ipdr session (global configuration)

To enable the CMTS application to add a session to the Internet Protocol Detail Record (IPDR) exporter, use the **ipdr session** command in global configuration mode. To remove the session, use the **no** form of this command.

ipdr session *session_id session_name session_descr*

no ipdr session *session_id*

Syntax Description

session_id	The unique IPDR session ID.
session_name	The session name. The name should not contain extra spaces.
session_descr	The description of the session.

Command Default

No sessions are added to the IPDR exporter. It depends on the status of the IPDR exporter. After configuring one session;if the status of exporter is started, then the session is started automatically.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command allows the user to add a session to the IPDR exporter. User should provide session ID, session name and session description for every session.

The **no** form of the command will remove a specific session. Once a session is removed, the template and other information associated with the session is also lost.

Note You can not update template details or other details when a session already created.

Examples

The following example adds a session to the Exporter.

```
Router# configure terminal
Router(config)#ipdr session  1 test no_descr
```

Related Commands

Command	Description
ipdr exporter start	Starts the IPDR exporter and connects to the collector.
show ipdr exporter	Displays information about the IPDR exporter state.
ipdr associate	Associates the IPDR collector with a session.

ipdr template

To add an Internet Protocol Detail Record (IPDR) template to the IPDR session on the Cisco CMTS, use the **ipdr template** command in global configuration mode. To remove the template, use the **no** form of this command.

ipdr template *session_id template_name*

no ipdr template *session_id template_name*

Syntax Description

session_id	Unique IPDR Session ID.
template_name	Template name.

Command Default

The IPDR template is not added to the IPDR session.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
12.2(33)SCG	A new template SERVICE-FLOW is added to the event-based and ad-hoc session types.

Usage Guidelines

This command allows the user to add an IPDR template to the desired session (based on session ID,) on the Cisco CMTS.

Note You can only add the system-supported templates. The list can be viewed by entering "**?**" at the command prompt.

Examples

The following example displays the **show running-config** command output of the configured IPDR sessions and types:

```
Router(config)# do show running-config | i ipdr

ipdr session 1 test test
ipdr session 2 event2 event2
ipdr session 3 ad-hoc3 ad-hoc3
ipdr type 1 time-interval 15
ipdr type 2 event
ipdr type 3 event
```

The following example shows the templates available in a timer-interval session.

```
Router# ipdr template 1 ?

  CM-STATUS       DOCSIS-CMTS-CM-REG-STATUS-TYPE template
  CM-US           DOCSIS-CMTS-CM-US-STATS-TYPE template
  DIAGLOG-DETAIL  DOCSIS-DIAG-LOG-DETAIL-TYPE template
  SAMIS-TYPE1     DOCSIS-SAMIS-TYPE-1 template
  SAMIS-TYPE2     DOCSIS-SAMIS-TYPE-2 template
  SPECTRUM        DOCSIS-SPECTRUM-MEASUREMENT-TYPE template
  TEST            Template for test
```

The following example shows how to add the SAMIS_TYPE1 template in a timer-interval session.

```
Router(config)# ipdr template 1 SAMIS-TYPE1
```

The following example shows how to view the templates available in an event-based session.

```
Router(config)# ipdr template 2 ?

  CM-STATUS       DOCSIS-CMTS-CM-REG-STATUS-TYPE template
  CPE-TYPE        DOCSIS-CPE-TYPE template
  DIAGLOG-DETAIL  DOCSIS-DIAG-LOG-DETAIL-TYPE template
  DIAGLOG-EVENT   DOCSIS-DIAG-LOG-EVENT-TYPE template
  DS-UTIL         DOCSIS-CMTS-DS-UTIL-STATS-TYPE template
  SAMIS           OSSI2.0 SAMIS template
  SERVICE-FLOW    SERVICE-FLOW-TYPE template
  TEST            Template for test
  TOPOLOGY        DOCSIS-CMTS-TOPOLOGY-TYPE template
  US-UTIL         DOCSIS-CMTS-US-UTIL-STATS-TYPE template
```

The following example shows how to view the templates available in an ad-hoc session.

```
Router(config)# ipdr template 3 ?

  CM-STATUS       DOCSIS-CMTS-CM-REG-STATUS-TYPE template
  CPE-TYPE        DOCSIS-CPE-TYPE template
  DIAGLOG-DETAIL  DOCSIS-DIAG-LOG-DETAIL-TYPE template
  DIAGLOG-EVENT   DOCSIS-DIAG-LOG-EVENT-TYPE template
  DS-UTIL         DOCSIS-CMTS-DS-UTIL-STATS-TYPE template
  SAMIS           OSSI2.0 SAMIS template
  SERVICE-FLOW    SERVICE-FLOW-TYPE template
  TEST            Template for test
  TOPOLOGY        DOCSIS-CMTS-TOPOLOGY-TYPE template
  US-UTIL         DOCSIS-CMTS-US-UTIL-STATS-TYPE template
```

Related Commands

Command	Description
ipdr exporter start	Starts the IPDR Exporter on the Cisco CMTS and connects to the collector.
show ipdr exporter	Displays information about the IPDR Exporter state on the Cisco CMTS.
ipdr session	Adds a session to the IPDR Exporter on the Cisco CMTS.

ipdr type

To configure the IPDR session type, use the **ipdr type** command in global configuration mode. The IPDR session types that can be defined using this command are event type, time-interval type, and the ad hoc type.

Use the **no** form of the command to reset the session type to the default "event" type.

ipdr type *session_id* [**ad-hoc** | **event** | **time-interval** *value*]

no ipdr type *session_id*

Syntax Description

session id	IPDR session ID. Range is from 1 to 255.
ad-hoc	The ad hoc session type.
event	The event session type.
time-interval *value*	The time-interval session type. Interval range is from 15 to 1440 minutes.

Command Default

The IPDR session type is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCD2	This command was introduced.

Usage Guidelines

This command allows the user to define the specific IPDR session type.

Note Once the IPDR session type is configured, the templates supported by this IPDR type are automatically associated with it.

Examples

The following example shows how to configure the IPDR “time-interval” session type for a time interval of 15 minutes.

```
Router> enable
Router# configure terminal
Router(config)# ipdr type 1 time-interval 15
```

Related Commands

Command	Description
cable ipdr cm-us-status interval	Displays a cable modem's upstream channel status information.
cable ipdr docs-spectrum interval	Sets the interval between different spectrum measurements' data for a CMTS.
cable ipdr diaglog interval	Sets the time interval between different diagnostic logs' data for a CMTS.
cable ipdr cm-status interval	Displays the CMTS and cable modem registration status information.

issu linecard abortversion

To abort or roll back the current image version on a single line card or multiple line cards to the previous version, use the **issu linecard abortversion** command in the privileged EXEC mode.

Note This command is used to abort or roll back the versions on redundant line cards only.

issu linecard abortversion all | *lc_slot*[*/subslot*] [**forced**]

Syntax Description

all	All redundant line cards.
lc_slot	The line card slot number.
subslot	The line card sub slot number.
forced	(Optional) The ISSU would ignore potential service outage and line card incompatibility errors and proceed with abortversion instead of stopping and error handling.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to roll back to prior image on working or primary line card on a single or multiple line cards to the previous versions.

Note The **issu linecard reloadversion** command is used to reload a line card with the original version of images.

The following example aborts the specific redundant line card's image version.

```
Router# configure terminal
Router(config)#issu linecard abortversion
```

Related Commands

Command	Description
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.

Command	Description
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single line card or multiple line cards.

issu linecard acceptversion

To accept the new image version on the working line card, use the **issu linecard acceptversion** command in the privileged EXEC mode.

issu linecard acceptversion *lc_slot*[*/subslot*]

Syntax Description

lc_slot	The line card slot number.
subslot	The line card sub slot number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to accept the new image version on the working line card. The command also indicates the completion of changing the image version for the specific line card and allows the ISSU of the next line card in the queue.

Examples

The following example indicates a command accepting the image version on the slot 7 of the line card.

```
Router# configure terminal
Router(config)#issu linecard acceptversion 7/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working/primary line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single line card or multiple line cards.

issu linecard changeversion

To start the upgrade or downgrade activity of the image version for a single working line card or multiple working line cards, use the **issu linecard changeversion** command in the privileged EXEC mode.

issu linecard changeversion {all | stop | *slot_1*[*/subslot_1*] … [*slot_n*[*/subslot_n*]]**} [forced]**

Syntax Description

all	All redundant line cards.
slot_1	The slot number for the first line card.
subslot_1	The sub slot number for the first line card.
slot_n	The slot number for the n^{th} line card.
subslot_n	The sub slot number for the n^{th} line card.
forced	(Optional) The ISSU would ignore potential service outage and line card incompatibility errors and proceed with changeversion instead of stopping and error handling.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to start the upgrade or downgrade activity of the image version for a single line card or multiple line cards. Here the line cards are of the primary or working type only.

Using the **all** option, you can change the image version of all the redundant line cards instead of specifying explicity each of the line card.

Using the **stop** option, you can abort or stop the version change process for a line card.

Examples

The following example displays the command and uses the **all** option.

```
Router# configure terminal
Router(config)#issu linecard changeversion all
```

The following example displays the command and uses the slot value of 6.

```
Router# configure terminal
Router(config)#issu linecard changeversion 6/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working/primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.

issu linecard loadversion

To load a specific image version on the primary line card, use the **issu linecard loadversion** command in the privileged EXEC mode.

issu linecard loadversion *slot*[/*subslot*]

Syntax Description

slot	The line card slot number.
subslot	The line card sub slot number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to load a specific image version on the working line card.

Examples

The following example shows the command that loads the image version on a line card with the slot number 7.

```
Router# configure terminal
Router(config)#issu linecard loadversion 7/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working/primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single line card or multiple line cards.

issu linecard prepareversion

To determine if the image version on the line card has to be upgraded or downgraded to the route processor's image version, use the **issu linecard prepareversion** command in the privileged EXEC mode.

issu linecard prepareversion *lc_slot*[/*subslot*] [**forced**]

Syntax Description

lc_slot	The line card slot number.
subslot	The line card sub slot number.
forced	(Optional) The ISSU would ignore potential service outage and line card incompatibility errors and proceed with prepareversion instead of stopping and error handling.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to check if the image version on the line card has to be upgraded or downgraded to the route processor's image version.

This command also checks if the line card has a valid redundancy configuration. If the line card does not have a valid configuration, then the user has to reload the line card using the **issu linecard reloadversion** command.

Examples

The following example shows the command executed for a line card with a slot value of 7.

```
Router# configure terminal
Router(config)#issu linecard prepareversion 7/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working/primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.

Command	Description
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single line card or multiple line cards.

issu linecard process stop

To stop the automatic line card ISSU process, use the **issu linecard process stop** command in privileged EXEC mode mode.

issu lineccard process stop

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

Use the **issu linecard process stop** command to interrupt the automatic ISSU process continuing to the next line card.

Starting Cisco IOS Release 12,2(33)SCG and later, **issu linecard process stop** is no longer supported on the Cisco CMTS router.

Associated Features

The **issu linecard process stop** command is associated with following features:

- *Cisco IOS In Service Software Upgrade Process*

Examples

The following example shows how to stop the ISSU process:

```
Router> enable
Router# issu linecard process stop
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working/primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.

Command	Description
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single line card or multiple line cards.

issu linecard reloadversion

To reload the new loaded image on a working or a primary line card, use the **issu linecard reloadversion** command in the privileged EXEC mode.

issu linecard reloadversion {original | target} all | *slot_1*[*/subslot_1*] … [*slot_n*[*/subslot_n*]]

Syntax Description

original	The original image version.
all	All redundant line cards.
slot_1	The slot number for the first line card.
subslot_1	The sub slot number for the first line card.
slot_n	The slot number for the n^{th} line card.
subslot_n	The sub slot number for the n^{th} line card.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to reload the new loaded image on a working or a primary line card.

This command can be used for the following line card conditions.

- Line cards that are not configured with redundancy, and do not support Minimal Disruptive Restart (MDR.)
- Line cards which are capable of line card redundancy which were rolled back due to an unsuccessful changeversion command.

Examples

The following example shows the command executed with the **original** keyword.

```
Router# configure terminal
Router(config)#issu linecard reloadversion original 8/0
```

The following example shows the command executed with the **target** keyword.

```
Router# configure terminal
Router(config)#issu linecard reloadversion target 8/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on working or primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.
issu linecard runversion	Runs the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single linecard or multiple line cards.

issu linecard runversion

To run the new loaded image on a working or a primary line card, use the **issu linecard runversion** command in the privileged EXEC mode.

issu linecard runversion *lc_slot*[*/subslot*] [**forced**]

Syntax Description

lc_slot	The line card slot number.
subslot	The line card sub slot number.
forced	(Optional) The ISSU would ignore potential service outage and line card incompatibility errors and proceed with runversion instead of stopping and error handling.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command allows the user to run the new loaded image on a working or a primary line card.

Examples

The following example displays the command executed to run the loaded image in the line card slot 7.

```
Router# configure terminal
Router(config)#issu linecard runversion 7/0
```

Related Commands

Command	Description
issu linecard abortversion	Rolls back to the prior image on the working/primary line card.
issu linecard acceptversion	Accepts the new image version on the working line card.
issu linecard loadversion	Loads a specific image version on the primary line card.
issu linecard prepareversion	Determines if the image version on the line card has to be upgraded or downgraded to the route processor's image version.
issu linecard reloadversion	Reloads the new loaded image on a working or a primary line card.
issu linecard changeversion	Starts the upgrade or downgrade activity of the image version for a single linecard or multiple line cards.

license feature evaluation disable

To disable an evaluation license for Cisco uBR-MC3GX60V and Cisco UBR-MC20X20V cable interface line cards on the Cisco uBR10012 router, use the **license feature evaluation disable** command in global configuration mode.

license feature evaluation disable {**DS_License** | **US_License** | **all**} **subslot** *slot*/*subslot*

Syntax Description

disable	Disables an evaluation license for a cable interface line card.
DS_License	Disables a downstream evaluation license for a cable interface line card.
US_License	Disables an upstream evaluation license for a cable interface line card.
all	Disables both downstream and upstream evaluation licenses for a cable interface line card.
subslot *slot*/*subslot*	• *slot*—Slot where the line card resides. The valid range is from 5 to 8. • *subslot*—Secondary slot number of the cable interface line card. The valid value is 0 or 1.

Command Default

A cable interface line card evaluation license is disabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Evaluation licenses are temporary and used to evaluate a feature set on a new line card. Ensure that an equivalent permanent license is installed on the Cisco CMTS before the evaluation license expires to avoid any service disruptions.

To obtain evaluation licenses from the Cisco licensing portal, go to: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y

Examples

The following example shows how to disable both downstream and upstream evaluation licenses for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation disable all subslot 5/0
```

The following example shows how to disable a downstream evaluation license for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation disable DS_License subslot 6/0
```

The following example shows how to disable an upstream evaluation license for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation disable US_License subslot 6/1
```

Related Commands

Command	Description
license feature evaluation enable	Enables an evaluation license for Cisco uBR-MC3GX60V and Cisco UBR-MC20X20V cable interface line cards.

license feature evaluation enable

To enable an evaluation license for Cisco uBR-MC3GX60V and Cisco UBR-MC20X20V cable interface line cards on the Cisco uBR10012 router, use the **license feature evaluation enable** command in global configuration mode.

license feature evaluation enable {**DS_License** | **US_License** | **all**} **subslot** *slot*/*subslot*

Syntax Description

enable	Enables an evaluation license for a cable interface line card.
DS_License	Enables a downstream evaluation license for a cable interface line card.
US_License	Enables an upstream evaluation license for a cable interface line card.
all	Enables both downstream and upstream evaluation licenses for a cable interface line card.
subslot *slot*/*subslot*	• *slot*—Slot where the cable interface line card resides. The valid range is from 5 to 8. • *subslot*—Secondary slot number of the cable interface line card. The valid value is 0 or 1.

Command Default

A cable interface line card evaluation license is not enabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Evaluation licenses are temporary and used to evaluate a feature set on a new cable interface line card. Ensure that an equivalent permanent license is installed on the Cisco CMTS router before the evaluation license expires to avoid any service disruptions.

To obtain evaluation licenses from the Cisco licensing portal, go to: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y

Examples

The following example shows how to enable both downstream and upstream evaluation licenses for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation enable all subslot 5/0
```

The following example shows how to enable a downstream evaluation license for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation enable DS_License subslot 6/0
```

The following example shows how to enable an upstream evaluation license for a cable interface line card on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# license feature evaluation enable US_License subslot 6/1
```

Related Commands

Command	Description
license feature evaluation disable	Disables an evaluation license for Cisco uBR-MC3GX60V and Cisco UBR-MC20X20V cable interface line cards.

logging cmts sea

To enable the logging of syslog messages to System Event Archive (SEA), use the **logging cmts sea** command from global configuration mode. To disable logging of syslog messages to SEA, use the **no** form of the command.

logging cmts sea [**syslog-level** [*level*]]

no logging cmts sea

Syntax Description

syslog-level *level*	(Optional) Configures the level of syslog messages inclusive of and above the specified level which will be stored in the SEA log file.
Possible values for level are: *level=emergencies*	Emergency security level indicates system is unusable. The default severity level for emergency syslog messages is 0.
level=alerts	Alerts severity level indicates that immediate action is needed. The default severity level for alerts syslog messages is 1.
level=critical	Critical severity level indicates the critical condition of the system. The default severity level for critical syslog messages is 2.
level=errors	Errors severity level indicates the error conditions. The default severity level for errors syslog messages is 3.
level=warnings	Warning severity level warns the network administrator. The severity level for warning syslog messages is 4.
level=notifications	Notification severity level indicates normal but significant condition of the system. By default severity level for syslog messages is configured as 'normal'. The default severity level for notification syslog messages is 5.
level=informational	Informational severity level provides additional information about the system. The default severity level for informational syslog messages is 6.
level=debugging	Debugging severity level provides debugging messages. The default severity level for debugging syslog messages is 7.

Command Default

By default, storing of syslog messages to SEA log file is enabled, with the severity-level of syslog messages being set to 'notification'.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **logging cmts sea** command is used to enable the logging of syslog messages to SEA log file. To change the severity-level of syslog messages inclusive of and above the level to be stored in SEA log file, specify the command **logging cmts sea** [**syslog-level** *level*].

Examples

The following example shows how to enable logging of syslog messages to SEA log file on the Cisco uBR10012 router:

```
Router(config)# logging cmts sea
```

The following example shows how to disable logging of syslog messages to SEA log file on the Cisco uBR10012 router:

```
Router(config)# no logging cmts sea
```

The following example shows how to change the severity-level of syslog messages inclusive of and above the level being stored in the SEA log file:

```
Router(config)# logging cmts sea syslog-level warning
```

Related Commands

clear logging system	Clears the event records stored in the SEA.
copy logging system	Copies the archived system events to another location.
logging system	Enables or disables the SEA logging system.

mac-address

To modify the default MAC address of an interface to some user-defined address, use the **mac-address** command in interface configuration mode. To return to the default MAC address on the interface, use the **no** form of this command.

mac-address *ieee-address*

no mac-address *ieee-address*

Syntax Description

ieee-address	48-bit IEEE MAC address written as a dotted triple of four-digit hexadecimal numbers.

Defaults

The interface uses a default MAC address that is derived from the base address stored in the electrically erasable programmable read-only memory (EEPROM).

Command Modes

Interface configuration

Usage Guidelines

Be sure that no other interface on the network is using the MAC address that you assign.

There is a known defect in earlier forms of this command when the Texas Instruments Token Ring MAC firmware is used. This implementation is used by Proteon, Apollo, and IBM RTs. A host using a MAC address whose first two bytes are zeros (such as a Cisco router) will not properly communicate with hosts using that form of this command of TI firmware.

There are two solutions. The first involves installing a static Routing Information Field (RIF) entry for every faulty node with which the router communicates. If there are many such nodes on the ring, this may not be practical. The second solution involves setting the MAC address of the Cisco Token Ring to a value that works around the problem.

This command forces the use of a different MAC address on the specified interface, thereby avoiding the Texas Instrument MAC firmware problem. It is up to the network administrator to ensure that no other host on the network is using that MAC address.

Examples

The following example sets the MAC layer address, where *xx.xxxx* is an appropriate second half of the MAC address to use:

```
interface tokenring 0
 mac-address 5000.5axx.xxxx
```

The following example changes the default MAC address on the interface to 1111.2222.3333:

```
Router# configure terminal
Router(config)# interface fastethernet 2/1/1
Router(config-if)# mac-address 1111.2222.3333
```

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

main-cpu

To enter main-CPU redundancy configuration mode, so that you can configure the synchronization of the active and standby Performance Routing Engine (PRE1) modules, use the **main-cpu** command in redundancy configuration mode.

main-cpu

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values

Command Modes

Redundancy configuration (config-r)

Command History

Release	Modification
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)BC3	Support for the **switchover timeout** command was added.
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.

Usage Guidelines

When you enter main-CPU redundancy configuration mode, the prompt changes to the following:

```
Router(config-r-mc)#
```

After you enter main-CPU redundancy configuration mode, you can use the **auto-sync** command to specify which files are synchronized between the active and standby PRE1 modules. In Cisco IOS Release 12.2(11)BC3 and later releases, you can also use the **switchover timeout** command to specify the amount of time that the standby PRE1 module should wait when it first detects that the active PRE1 module is not active and when it initiates a switchover and becomes the active PRE1 module.

To leave main-CPU redundancy configuration mode and to return to redundancy configuration mode, use the **exit** command.

Examples

The following example shows how to enter main-CPU redundancy mode and the commands that are available there:

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

Main Cpu redundancy configuration commands:
  auto-sync   Sync elements
  exit        Exit from main-cpu configuration mode
  no          Negate a command or set its defaults
  switchover  Configuration of switchover
```

```
Router(config-r-mc)#
```

Related Commands

Command	Description
associate slot	Logically associate slots for APS processor redundancy
auto-sync	Configures which files are synchronized between the active and standby PRE1 modules.
redundancy	Enters redundancy configuration mode.
switchover timeout	Configures the switchover timeout period of the PRE1 module.

maintenance-mode

To configure the PRE1 modules on the router for maintenance mode, use the **maintenance-mode** command in redundancy configuration mode. To return to normal operations, use the **no** form of this command.

maintenance-mode

no maintenance-mode

Syntax Description

This command has no keywords or arguments.

Command Default

Normal operations (**no maintenance-mode**)

Command Modes

Redundancy configuration

Command History

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

Usage Guidelines

When the Cisco uBR10012 router is configured with redundant PRE1 modules, the active PRE1 module automatically synchronizes the configuration, network state information, and other information with the standby PRE1 module, so that if a switchover occurs, the standby module can restore normal operations quickly. You can use the **maintenance-mode** command to disable this automatic synchronization of the PRE1 modules, and to disable the reporting of any faults on the standby module to the active module.

Note The **maintenance-mode** command disables the ability of the Cisco uBR10012 router to switchover PRE1 modules and should be used only while upgrading the router or troubleshooting network problems.

Examples

The following example shows how to disable the automatic PRE1 module synchronization on the Cisco uBR10012 router and enter maintenance mode:

```
Router# config t
Router(config)# redundancy
Router(config-r)# maintenance-mode
Router(config-r)# exit
Router(config)#
```

The following example shows how to leave maintenance mode and return to normal operations, which includes the automatic synchronization of the PRE1 modules:

```
Router# config t
Router(config)# redundancy
Router(config-r)# no maintenance-mode
Router(config-r)# exit
Router(config)#
```

Related Commands

Command	Description
auto-sync	Configures which files are synchronized between the active and standby PRE1 modules.
redundancy	Enters redundancy configuration mode.

match rule

To configure the match rule, rule priority and related action in the selected cable multicast authorization profile, use the **match rule** command in interface configuration mode. To disable a cable multicast authorization profile match, use the **no** form of this command.

match rule [*ipv4* | *ipv6*] [*source-prefix*] [*group-prefix]* **priority** [*priority-value*] [*permit* | *deny*]

no match rule [*ipv4/ipv6*] [*source-prefix*] [*group-prefix]* **priority** [*priority-value*] [*permit/deny*]

Syntax Description

match rule [*ipv4* | *ipv6*]	Specifies the matching source rule. **Note** Though CLI allows IPv6 to be configured, only IPv4 is supported in the CMTS.
source-prefix	(Optional) Specifies the matching source address prefix. Example: 223.1.1.1/16
group-prefix	(Optional) Specifies the matching group address prefix. Example: 223.1.1.1/16
priority [*priority-value*]	Specifies the priority of the cable multicast authorization profile. Priority value range is: 0-255.
permit	The argument *permit* allows specified packets to be forwarded.
deny	The argument *deny* allows to specified packets to be rejected.

Command Default

Cable multicast authorization is disabled.

Command Modes

Interface configuration—cable interface only (config-mauth)

Command History

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

Usage Guidelines

This command specifies the cable multicast authorization profile match to be used.

Examples

The following example shows how to use the selected multicast authorization profile match:

```
Router(config-mauth)# match rule rule1
```

Related Commands

Command	Description
cable multicast authorization enable default-action	This command enables the cable multicast authorization features. If the multicast authorization feature is disabled, all defined authorization profiles are ineffective.
cable multicast authorization profile-name	Defines the cable multicast authorization profile.
show cable multicast authorization	Displays the list of defined multicast authorization profiles and all CMs associated with corresponding profiles.

member subslot

To configure the redundancy role of a line card, use the **member subslot** command in line card redundancy group mode.

member subslot *slot/subslot* {**primary** | **secondary**}

no member subslot *slot/subslot* {**primary** | **secondary**}

Cisco uBR10012 Universal Broadband Routers

member subslot *slot/subslot* {**protect** [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

no member subslot *slot/subslot* {**protect** [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

Syntax Description

slot	Slot number of the line card in the chassis.
subslot	Slot number of the line card in the chassis.
primary | **secondary**	Configures the redundancy role of the line card. • **primary**—Active line card. • **secondary**—Standby line card.
protect	Specifies the protect slot in the line card group.
config *slot/subslot*	(Optional) Specifies the appropriate working interface configuration that is used for the protect interface when a switchover occurs.
rf-power	(Optional) Specifies the RF power output level on an integrated upconverter.
rf-connector *rfconnector-value*	(Optional) Specifies the RF connector in the protect line card. The default value is *all*.
hccp-delta *diff-pwr*	When using N+1 Hotstandby Connection-to-Connection Protocol (HCCP) redundancy, the protect interface adds the *diff-pwr* value to the current power value of the working interface when a switchover occurs. This allows the router to accommodate relative differences between the RF power levels in working and protect interfaces. The valid value for *diff-pwr* ranges from –12 to +12 dBmV.
hccp-override *override-pwr*	When using N+1 HCCP redundancy, the protect interface uses the override power value instead of the power value of the working interface when a switchover occurs. This allows the router to accommodate absolute differences between the RF power levels in working and protect interfaces. The valid value for *override-pwr* ranges from 45 to 63 dBmV. **Note** The official range for acceptable power levels in the DOCSIS specification is 50 to 61 dBmV. Cisco cable interfaces exceed the DOCSIS standard, but power levels outside the DOCSIS standards should be used only in lab and test environments.
working	Specifies the working slot in the line card group.
rfsw-slot *slot-value*	(Optional) Specifies the RF switch slot for the working line card.

revertive	Specifies the revert operation on the protect card.
reverttime *value*	Specifies the time interval for the revert operation in minutes. If you specify the time interval as 30 minutes, the protect card switches back to the protect mode after 30 minutes.

Command Default

None

Command Modes

Line card redundancy group

Command History

Release	Modification
12.2(28)SB	This command was introduced for the Cisco 10000 series routers.
12.3(23)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(33)SCA	Support for the following keywords was removed in Cisco IOS Release 12.2(33)SCA and later releases: • **revertive** • **reverttime** **Note** Use the **revertive** command in line card redundancy group mode to enable the revert operation on a protect card in Cisco IOS Release 12.2(33)SCA and later releases.
12.2(33)SCC4	Support for the following keywords was added in Cisco IOS Release 12.2(33)SCC4 for Cisco uBR10012 routers: • **rf-power** • **rf-connector** • **hccp-delta** • **hccp-override**
12.2(33)SCE	The **config** option of the command was made the default. When more than one working line cards are configured, the config option is automatically applied to the first working card.

Usage Guidelines

The primary line card must be the first line card configured and must occupy subslot 1. The secondary line card must be the second line card configured and must occupy subslot 0. Only one primary line card and one secondary line card can be configured.

Note Configuration changes to the working line card cause the upstream links on the protect line card to flap. This is applicable only to Cisco uBR10012 routers.

Examples

The following example shows how to create a line card group number 1 for one-to-one line card redundancy. It also specifies the line card in subslot 1 as the primary (active) line card, and the line card in subslot 0 as the secondary (standby) line card.

```
Router# configure terminal
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
```

Note The rest of the examples listed here are only applicable to Cisco uBR10012 routers.

The following example shows how to configure a protect interface to add 3 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-delta 3
```

The following example shows how to configure a protect interface to use an RF power level of 48 dBmV instead of the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-override 48
```

The following example shows how to configure a rf-connector 3 on a protect interface to add 5 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power rf-connector 3 hccp-delta 5
```

Related Commands

Command	Description
linecard-group	Creates a line card group for one-to-one line card redundancy.
redundancy	Enters redundancy mode.
show redundancy linecard	Displays information about a redundant line card or line card group.

method

To select the method the CMTS uses to determine the load, use the **method** command in the config-lb-group configuration mode. To reset the method, use the **no** form of this command.

method {**modems | service-flows | utilization**} {**us-method** {**modems | service-flows | utilization**}

no method

Syntax Description

modems	Specifies the load balancing method for the number of modems on the CMTS.
service-flows	Specifies the load balancing method for the number of service flows on the CMTS.
utilization	Specifies the load balancing method for the interface utilization on the CMTS.
us-method {**modems	service-flows	utilization**}	Specifies the load balancing method for upstream (US) channels on modems, service-flows, or utilization.

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

The upstream channel uses the same method as the downstream channel. Change the method of the upstream channel using the **method** command.

Examples

The following example shows how to select the method the CMTS uses to determine the load, using the **method** 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)# method modems us-method service-flows
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.

microcode (uBR10012)

To reload the microcode software images on a Parallel eXpress Forwarding (PXF) processor or on all line cards that support downloadable microcode, use the **microcode** command in global configuration mode.

microcode {**pxf** *filename* | **reload**}

Syntax Description

pxf	Reloads the microcode for the PXF processors on the Performance Routing Engine (PRE1) module.
filename	Specifies the microcode software image for the PXF processors by device name and filename.
reload	Reloads the microcode for all PRE1 modules and other line cards that support downloadable microcode software images.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)XF1	This command was introduced for the Cisco uBR10012 router.

Usage Guidelines

By default, the Cisco uBR10012 router automatically loads all required microcode on to the PXF processors and other line cards when it loads the Cisco IOS software image. Also, the PRE1 module automatically reloads the microcode on a card when certain faults occur, allowing the card to recover from the fault.

You can reload the microcode on the PRE1 module or on all line cards that support downloadable microcode by using the **microcode** command. Typically, this is not needed and should be done only upon the advice of Cisco TAC or field service engineers.

Tip You can also reload the microcode on the PXF processors or on all cards using the **microcode reload** command in privileged EXEC mode. In particular, use the **microcode reload** command to reload the PXF processors with the default microcode that was loaded along with the Cisco IOS software image.

Examples

The following example shows how to reload the microcode on all PRE processors and line cards that support downloadable microcode:

```
Router# configure terminal
Router(config)# microcode reload
Reload microcode? [confirm] yes

00:49:41: Downloading Microcode: file=system:pxf/ubr10k-ucode.1.2.3,
```

```
version=1.1.0, description=Release Software created Wed 17-Jul-02 16:58

<<list of interfaces going down or coming up>>

00:49:42: !!pxf clients started, forwarding code operational!!

Router(config)#
```

The following example shows how to reload the microcode on the PXF processors on the PRE1 module, using a specific image that is stored in the Flash memory:

```
Router# configure terminal
Router(config)# microcode pxf flash:pxf/ubr10k-ucode.122.1.2.3
Reload microcode? [confirm] yes

1d04h: Downloading Microcode: file=flash:pxf/ubr10k-ucode.122.1.2.3, version=122.1.2.3,
description=Release Software created Thu 17-Oct-02 11:33

<<list of interfaces going down or coming up>>

1d04h: !!pxf clients started, forwarding code operational!!

Router(config)#
```

Related Commands

Command	Description
hw-module reset	Resets a particular PRE1 module or a particular line card.
microcode reload	Reloads the microcode software images on one or all line cards that support downloadable microcode.
show pxf microcode	Displays display identifying information for the microcode being used on the PXF processors.

microcode reload (uBR10012)

To reload the microcode software images on one or all line cards that support downloadable microcode, use the **microcode reload** command in privileged EXEC mode.

microcode reload {**all** | **pxf** [*device:*[*filename*]]}

Syntax Description

all	Reloads the microcode for all Performance Routing Engine (PRE1) modules and other line cards that support downloadable microcode software images.
pxf	Reloads the microcode for the Parallel eXpress Forwarding (PXF) processors on the PRE1 module.
device:[*filename*]	(Optional) Loads the PXF processors with the microcode software image that has the specific filename on the specific device. If no filename is specified, the first image found on the device is loaded by default.

Command Default

For **microcode reload pxf**, defaults to loading the microcode image that was originally loaded when the Cisco IOS software image was loaded.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(1)XF1	This command was introduced for the Cisco uBR10012 router.

Usage Guidelines

By default, the Cisco uBR10012 router automatically loads all required microcode on to the PXF processors and other line cards when it loads the Cisco IOS software image. Also, the PRE1 module automatically reloads the microcode on a card when certain faults occur, allowing the card to recover from the fault.

You can reload the microcode on the PRE1 module or on all line cards that support downloadable microcode by using the **microcode reload** command. Typically, this is not needed and should be done only upon the advice of Cisco TAC or field service engineers.

Tip You can also reload the microcode on the PXF processors or on all cards using the **microcode** command in global configuration mode.

Examples

The following example shows how to reload the microcode on all PRE processors and line cards that support downloadable microcode:

```
Router# microcode reload all
Reload microcode? [confirm] yes
```

```
00:49:41: Downloading Microcode: file=system:pxf/ubr10k-1-ucode.122.1.0, version=122.1.0,
description=Release Software created Wed 17-Jul-02 16:58

<<list of interfaces going down or coming up>>

00:49:42: !!pxf clients started, forwarding code operational!!

Router#
```

The following example shows a typical list of devices that you can use when loading microcode for the PXF processors. This list might vary, depending on whether a standby PRE1 module is installed and depending on the version of Cisco IOS software being used.

```
Router# microcode reload pxf ?

   bootflash:      location of microcode
   disk0:          location of microcode
   disk1:          location of microcode
   flash:          location of microcode
   ftp:            location of microcode
   null:           location of microcode
   nvram:          location of microcode
   rcp:            location of microcode
   scp:            location of microcode
   sec-bootflash:  location of microcode
   sec-disk0:      location of microcode
   sec-disk1:      location of microcode
   sec-nvram:      location of microcode
   sec-slot0:      location of microcode
   sec-slot1:      location of microcode
   slot0:          location of microcode
   slot1:          location of microcode
   system:         location of microcode
   tftp:           location of microcode
   <cr>

Router#
```

The following example shows how to reload the microcode on the PXF processors on the PRE1 module, using a specific image that is stored in the Flash memory:

```
Router# microcode reload pxf flash:pxf/ubr10k-1-ucode.122.1.0.4
Reload microcode? [confirm] yes

3d00h: Downloading Microcode: file=flash:pxf/ubr10k-1-ucode.122.1.0.4, version=122.1.0.4,
description=Release Software created Thu 27-Jun-02 16:05

<<list of interfaces going down or coming up>>

3d00h: !!pxf clients started, forwarding code operational!!

Router#
```

Related Commands

Command	Description
hw-module reset	Resets a particular PRE1 module or a particular line card.
microcode	Reloads the microcode software images on one or all line cards that support downloadable microcode.
show pxf microcode	Displays display identifying information for the microcode being used on the PXF processors.

mode (redundancy)

To configure the redundancy mode of operation, use the **mode** command in redundancy configuration mode.

Cisco 7304 Router

mode {**rpr** | **rpr-plus** | **sso**}

Cisco 7500 Series Routers

mode {**hsa** | **rpr** | **rpr-plus** | **sso**}

Cisco 10000 Series Routers

mode {**rpr-plus** | **sso**}

Cisco 12000 Series Routers

mode {**rpr** | **rpr-plus** | **sso**}

Cisco uBR10012 Universal Broadband Router

mode {**rpr-plus** | **sso**}

Syntax Description

rpr	Route Processor Redundancy (RPR) redundancy mode.
rpr-plus	Route Processor Redundancy Plus (RPR+) redundancy mode.
sso	Stateful Switchover (SSO) redundancy mode.
hsa	High System Availability (HSA) redundancy mode.

Command Default

The default mode for the Cisco 7500 series routers is HSA.
The default mode for the Cisco 7304 router and Cisco 10000 series routers is SSO.
The default mode for the Cisco 12000 series routers is RPR.
The default mode for the Cisco uBR10012 universal broadband router is SSO.

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(22)S	SSO support was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support was added for the Cisco 7304 router. The Cisco 7500 series router is not supported in Cisco IOS Release 12.2(20)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCE	This command was modified in Cisco IOS Release 12.2(33)SCE. The **rpr-plus** keyword was removed.

Usage Guidelines

The mode selected by the **mode** command in redundancy configuration mode must be fully supported by the image that has been set into both the active and standby Route Processors (RPs). A high availability image must be installed into the RPs before RPR can be configured. Use the **hw-module slot image** command to specify a high availability image to run on the standby RP.

For Cisco IOS Release 12.2(33)SCA on the Cisco 10000 series routers and the Cisco uBR10012 universal broadband router, the use of SSO redundancy mode is recommended because RPR+ redundancy mode is being removed. If you enable RPR+ redundancy mode, you may see the following message:

```
*******************************************************
* Warning, The redundancy mode RPR+ is being deprecated *
* and will be removed in future releases. Please change *
* mode to SSO:                                          *
*     redundancy                                        *
*        mode sso                                       *
*******************************************************
```

Examples

The following example configures RPR+ redundancy mode on a Cisco 12000 series or Cisco 1000 series router:

```
Router# mode rpr-plus
```

The following example sets the mode to HSA on a Cisco 7500 series router:

```
Router# mode hsa
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby Route Processor (RP).
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces the standby Route Processor (RP) to assume the role of the active RP.
show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

modular-host subslot

To specify the modular-host line card that will be used for DOCSIS 3.0 downstream or downstream channel bonding operations, use the **modular-host subslot** command in controller configuration mode. To remove the modular-host line card used for DOCSIS 3.0 downstream or downstream channel bonding operations, use the **no** form of this command.

modular-host subslot *slot/subslot*

no modular-host subslot *slot/subslot*

Syntax Description

slot/subslot	The location of the modular-host line card.

Command Default

No modular-host line card is configured for DOCSIS 3.0 downstream or downstream channel bonding operations.

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

This command specifies the modular-host line card for DOCSIS 3.0 downstream or downstream channel bonding operations. This applies to the cable interface line card (for example, the Cisco uBR10-MC5X20S-D line card) that is used for these operations. The Wideband SPA itself does not support DOCSIS 3.0 downstream channel bonding operations.

Note A maximum of 3 SPA controllers can be hosted on a single cable interface line card.

Examples

The following example shows how to configure the modular-host line card for DOCSIS 3.0 downstream channel bonding operations for the Wideband SPA located in slot/subslot/bay 1/0/0:

```
Router(config)# controller modular-cable 1/0/0
Router(config-controller)# modular-host subslot 7/0
```

Related Commands

Command	Description
annex modulation	Sets the annex and modulation for the Wideband SPA.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel.

Command	Description
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.
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 cable downstream channel-id	Assigns a downstream channel ID to an RF channel.

monitoring-basics

To specify the type of monitoring for subscriber traffic management on a Cisco CMTS router, use the **monitoring-basics** command in enforce-rule configuration mode. To disable the selected monitoring, use the **no** form of this command.

monitoring-basics {**legacy** | **peak-offpeak**} {**docsis10** | **docsis11**}

no monitoring-basics {**legacy** | **peak-offpeak**} {**docsis10** | **docsis11**}

Syntax Description

legacy	Provides only one threshold and one monitoring duration.
peak-offpeak	Allows the selection of two peak durations within a day.
docsis10	Specifies application of the enforce-rule to DOCSIS 1.0 cable modems.
docsis11	Specifies application of the enforce-rule to DOCSIS 1.1 cable modems.

Command Default

The default for this command is **legacy** and **docsis10**.

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

Legacy monitoring (using the **legacy** keyword) occurs 24 hours a day, with no distinction between peak and offpeak hours. The available monitoring duration is between 10 minutes and 31 days.

Use the **peak-offpeak** keyword to set up monitoring duration and threshold for first peak, second peak, and offpeak monitoring. Each one can be different. After setting up first peak and second peak durations, the remaining hours are treated as offpeak. Monitoring happens during offpeak hours if the offpeak duration and threshold are defined. Monitoring duration is between 60 minutes and 23 hours.

Examples

The following example shows configuration of peak-offpeak monitoring for DOCSIS 1.1 cable modems:

```
Router(enforce-rule)# monitoring-basics peak-offpeak docsis11
```

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.

Command	Description
duration	Specifies the time period and sample rate to be used for monitoring subscribers.
peak-time1	Specifies peak and offpeak monitoring times.
qos-profile registered	Specifies the registered QoS profile that should be used for this enforce-rule.
qos-profile enforced	Specifies a QoS profile that should be enforced when users violate the registered QoS profiles.
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.

monitoring-duration

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

To specify the time period and sample rate to be used for monitoring subscribers, use the **monitoring-duration** command in enforce-rule configuration mode. To reset an enforce-rule to its default values, use the **no** form of this command.

monitoring-duration *minutes* [**sample-rate** *minutes*]

no monitoring-duration

Syntax Description

minutes	Specifies the time (in minutes). The valid range is 10 to 10080, with a default of 360 (6 hours).
sample-rate *minutes*	(Optional) Rate of sampling, in minutes. The valid range is 1 to 30, with a default value of 15.

Defaults

The **monitoring-duration** value defaults to 360 minutes (6 hours), and the **sample-rate** value defaults to 15 minutes.

Command Modes

Enforce-rule configuration (enforce-rule)

Command History

Release	Modification
12.2(15)BC1	This command was introduced.
12.2(15)BC2	The minimum **sample-rate** was reduced to 1 minute. Also, the **sample-rate** is not allowed to be set to a value greater than the **monitoring-duration** period. If you attempt to do so, the command is ignored and both parameters remain set to their current values.
12.3(9a)BC	This command was replaced by the **duration** command.

Usage Guidelines

The **sample-rate** *minutes* must be less than or equal to the **monitoring-duration** *minutes* period.

When you enable an enforce-rule, the Cisco CMTS router periodically checks the bandwidth being used by subscribers, to determine whether any subscribers are consuming more bandwidth than that specified by their registered QoS profile. The Cisco CMTS router keeps track of the subscribers using a sliding window that begins at each sample-rate interval and continues for the monitoring-duration period.

For example, with the default sample-rate interval of 15 minutes and the default monitoring-duration window of 360 minutes, the Cisco CMTS router samples the bandwidth usage every 15 minutes and determines the total bytes transmitted at the end of each 360-minute period. Each sample-rate interval begins a new sliding window period for which the Cisco CMTS router keeps track of the total bytes transmitted.

Note The **sample-rate** interval must be less than or equal to the **monitoring-duration** period. If you attempt to set the sample-rate interval to a value greater than the monitor-duration period, the command is ignored and the parameters are unchanged.

When you change the configuration of a currently active enforce-rule, that rule begins using the new configuration immediately to manage the cable modems tracked by this enforce-rule.

For more information about the Subscriber Traffic Management feature and to see an illustration of a sample monitoring window, refer to the Subscriber Traffic Management for the Cisco CMTS Routers feature document on Cisco.com.

Examples

The following example shows an enforce-rule being configured for a monitoring-duration period that is 20 minutes in length, with a sampling rate of every 10 minutes:

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# monitoring-duration 20 sample-interval 10
```

The following example shows the error message that is displayed when the **sample-rate** interval is configured to be greater than the **monitoring-duration** period. In this situation, the command is ignored and the parameters remain unchanged.

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# monitoring-duration 20 sample-interval 30

Monitoring duration cannot be less than the Sampling interval -- so the values
would remain unchanged
```

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.
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.
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.

name

To specify the name of the CMTS tag, use the **name** command in the cmts-tag configuration mode. To remove the name, use the **no** form of this command.

name *tag-name*

no name *tag-name*

Syntax Description

tag-name	Name of the CMTS tag. The configured name is added to the DOCSIS load balancing group and policies.

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 give name to a CMTS tag using the **name** command:

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

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.

network

To configure the DHCP address pool with the specified *network-number* and subnet *mask*, which are the DHCP *yiaddr* field and Subnet Mask (DHCP option 1) field, use the **network** command in global configuration mode. To remove this configuration, use the **no** form of this command.

network *network-number* [*mask*]

no network *network-number* [*mask*]

Syntax Description

network-number	The DHCP *yiaddr* field.
mask	Subnet Mask (DHCP option 1). If you do not specify the *mask* value, it is supported to 255.255.255.255.

Command Default

DHCP settings are not configured by default.

Command Modes

DHCP configuration

Command History

Release	Modification
Release 12.2(4)BC1	Supoported on the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers.

Usage Guidelines

This command requires that you first use the **dhcp ip dhcp pool name** command in global configuration mode to enter DHCP configuration mode.

Note To create an address pool with a single IP address, use the **host** command instead of **network**.

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

- *DHCP and ToD Servers on the Cisco CMTS*

Examples

The following example illustrates use of the **network** command with the **ip dhcp pool name** command.

```
Router# configure terminal
Router(config)# ip dhcp pool name platinum
Router(dhcp-config)# network 10.10.10.0 255.255.0.0
Router(dhcp-config)#
```

Related Commands

ip dhcp pool name	Creates a DHCP address pool and enters DHCP pool configuration file mode.

nls

To enable Network Layer signaliing (NLS) functionality, use the **nls** command in global configuration mode. To disable NLS functionality, use the **no** form of this command.

nls [**authentication**]

no nls [**authentication**]

Syntax Description

authentication	(Optional) Enables NLS protocol security authentication.

Command Default

Disabled.

Command Modes

Global configuaration

Command History

Release	Modification
12.3(21a)BC3	This command was introduced.

Usage Guidelines

It is recommended that NLS message authentication is enabled all the time.

Examples

The following example shows nls enabled on a router:

```
router (config)# nls
```

Related Commands

Command	Description
cpd	Enables the CPD feature.
nls ag-id auth-key	Configures an Authorization Group Identifier (AG ID) for CMTS.
nls resp-timeout	Configures NLS response timeout.

nls ag-id auth-key

To configure an Authorization Group Identifier (AG ID) for CMTS, use the **nls ag-id auth-key** command in global configuration mode. To disable the AG ID, use the **no** form of this command.

nls ag-id auth-key

no nls ag-id auth-key

Syntax Description

ag-id number	Authorization Group Identifier. The valid range is 1-4294967294.
auth-key char	Authentication key provisioned on CMTS. The valid range is 20-64.

Command Default

Disabled

Command Modes

Global configuaration

Command History

Release	Modification
12.3(21a)BC3	This command was introduced.

Examples

The following example shows configuring the AG ID:

```
Router(config) # nls ag-id 345 auth-key 54
```

Related Commands

Command	Description
cpd	Enables CPD.
nls	Enables Network Layer signaliing (NLS) functionality.
nls resp-timeout	Configures NLS response timeout.

nls resp-timeout

To configure the NLS response timeout, use the **nls resp-timeout** command in global configuration mode. To disable CPD, use the **no** form of this command.

nls resp-timeout *timeout number*

no nls resp-timeout *timeout number*

Syntax Description

timeout number	Controls the time CTMS will wait before getting a response for an NLS information request. The valid range is 1-60 seconds. Upon a response timeout, the CPD message is dropped.

Command Default

The default timeout is 1 second.

Command Modes

Global configuration

Command History

Release	Modification
12.3(21a)BC3	This command was introduced.

Examples

The following example shows configuring the NLS response timeout:

```
Router(config)#nls rssp-timeout 35
```

Related Commands

Command	Description
cpd	Enables CPD.
nls	Enables Network Layer signalling (NLS) functionality.
nls ag-id auth-key	Configures an Authorization Group Identifier (AG ID) for CMTS.

oui

To configure the Organizational Unique Identifier (OUI) of the CM for the CMTS tag, use the **oui** command in the cmts-tag configuration mode. To remove the configured OUI from the CMTS tag, use the **no** form of this command.

[**exclude**] **oui** *oui-of-CM*

no oui *oui-of-CM*

Syntax Description

exclude	(Optional) Configures the tag to exclude the specified OUI.
oui-of-CM	MAC address prefix of the vendor.

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 OUI for the CMTS tag using the **oui** command:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# oui 00.1a.c3
```

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.

output-rate

Note Starting with Cisco IOS Release 12.2(33)SCG, the **output-rate** command is not supported on the Cisco uBR10012 router.

To specify a custom-defined output line rate to a WAN interface instead of the default output line rate, use the **output-rate** command in interface configuration mode. Use the **no** form of this command to use the default output line rate.

output-rate *rate*

no output-rate

Syntax Description

rate	Output rate to the WAN interface, in kilobits per second. Valid values range from 1 to 1,000,000.

Command Default

Gigabit Ethernet output line rate is 1,000,000 kbps.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCC	This command was introduced.
12.2(33)SCG	Support for this command was removed for the Cisco uBR10012 router.

Usage Guidelines

This command specifies a custom-defined output line rate for the WAN interface.

Starting with Cisco IOS Release 12.2(33)SCG, the **output-rate** command is not supported and the value 10,000 is used for the output line rate on a Cisco uBR10012 router.

Examples

The following example shows how to specify a custom-defined output line rate for the WAN interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# output-rate 100
```

Related Commands

Command	Description
show running-config interface gigabitethernet	Displays the configuration settings for the specified Gigabit Ethernet interface.
show interfaces gigabitethernet	Displays the status and configuration settings for Gigabit Ethernet interfaces.

override

To override the Type/Length/Value (TLV) or SNMP when assigning a restricted load balancing group (RLBG) to CM, use the **override** command in the cmts-tag configuration mode. To reenable the TLV or SNMP when assigning a RLBG to CM, use the **no** form of this command.

override

no override

Command Default

TLV or SNMP are effective when assigning a RLBG to CM.

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 override the TLV or SNMP when assigning a RLBG using the **override** command:

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

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.
cable tag	Configures a tag for a DOCSIS load balancing group on the CMTS.

option

To create a DOCSIS configuration file that specifies vendor-specific information fields, or other options that are not available through the other **cable config-file** commands, use the **option** command in cable config-file configuration mode. To remove the entry for this option, use the **no** form of this command.

option *n* [**instance** *inst-num*] {**ascii** *string* | **hex** *hexstring* | **ip** *ip-address*}

no option *n*

Syntax Description

n	Specifies the configuration file option code. Valid range is 5 to 254. **Note** Certain values between 5 and 254 are not allowed. See Table 0-30 for more information.
instance *inst-num*	(Optional) Specifies the instance of this option, so that you can give the same option multiple times. Valid range is 0 to 255.
ascii *string*	Specifies that the data is a network verification tool (NVT) ASCII string. If the string contains white space, you must surround it with quotation marks.
hex *hexstring*	Specifies the data as a raw hexadecimal string. Each byte in the hexadecimal string is two hexadecimal digits—each byte can be separated by a period, colon, or white space. A maximum of 254 bytes can be specified. **Note** The **hex** option must be used to specify the data in the DOCSIS Type/Length/Value (TLV) format when using the vendor-specific option (**option 43**).
ip *ip-address*	Specifies an IP address.

Command Default

No default behaviors or values

Command Modes

Cable config-file configuration

Command History

Release	Modification
12.1(2)EC1	This command was introduced.
12.2(4)BC1	Support was added to the Release 12.2 BC train.

Usage Guidelines

The DOCSIS specification provides for a great many options and parameters in the DOCSIS configuration files. In particular, it allows unspecified vendor-specific options that can vary from vendor to vendor and from model to model. To create a DOCSIS configuration file that references these options, use the **option** command.

The **option** command allows you to specify configuration file parameters that are not defined by the other **cable config-file** options. These options are defined in the DOCSIS Radio Frequency (RF) Interface Specification. However, certain options are not allowed because they are either reserved for DOCSIS use or because they are specified using other **cable config-file** commands.

Table 0-30 lists the options that cannot be specified by the **cable config-file option** command. Where applicable, the table shows the **cable config-file** command you can use to specify that option.

Table 0-30 Invalid Option Codes for the cable config-file option Command

Option	Description	Cable Config-File Command
5, 6, 7, 20	Internal Configuration File Options	N/A
9	Software Upgrade Filename	download
12	Modem IP Address	N/A
13	Service Not Available Response	N/A
17	Baseline Privacy Interface Configuration	privacy
18	Maximum Number of CPE devices	cpe max
19	TFTP Server Timestamp	timestamp
21	Software Upgrade TFTP Server	download

Note For complete information on the other parameters and fields in DOCSIS configuration files, see Appendix C in the *DOCSIS 1.1 Radio Frequency (RF) Interface Specification*, available on the DOCSIS Cable Labs official web site at http://www.cablemodem.com/

Using Option 43 (Vendor-Specific Information Fields)

The most common use of the **cable config-file option** command is to specify vendor-specific information field values, which vendors use to implement features that are unique to their products. In this case, the value for *n* must be 43.When you use the vendor-specific option (**option 43**), you must specify the data using the **hex** option.

The hexadecimal data must be presented in the DOCSIS Type/Length/Value (TLV) format, where the first byte specifies the suboption type, the second byte specifies the length of the data, and the remaining bytes specify the data itself. The exact meaning of the suboption type and data values is defined by each vendor.

For example, Cisco CMs support a vendor-specific suboption (128) that instructs the CM to download and execute a Cisco IOS configuration file. The data for this suboption is the fully qualified path name of the Cisco IOS configuration file on the TFTP server. Other vendors, however, could define vendor-specific suboption 128 to have a totally different function.

To ensure that a vendor-specific option is executed only by equipment that supports that option, the vendor ID must always be the first part of the data in an **option 43** command. The suboption number for the vendor ID function is **08**, and the data is the three byte Organization Unique Identifier (OUI) for that vendor, as issued by the Institute of Electrical and Electronics Engineers (IEEE).

The vendor could have defined a global OUI for all of their equipment, or they could have requested a separate OUI ID for different products or family of products. For example, the global OUI for Cisco equipment is **00 00 0C**.

Note Each **option 43** command must specify one and only one vendor ID, and the vendor ID must be the first TLV in the **hex** data string.

Example of Constructing an Option 43 Command

For example, to create a vendor-specific option that downloads a Cisco IOS configuration file, you would create a hexadecimal data string that first contains suboption 8, to specify the vendor ID in TLV format. You would then add the hexadecimal string that contains suboption 128, to specify the filename for the configuration file to be downloaded, in TLV format.

The TLV for the Cisco vendor ID would be **08:03:00:00:0C**, where **08** is the suboption type, **03** is the length, and **00:00:0C** is the Cisco OUI vendor ID. If the Cisco IOS filename is **ios.cfg**, the second TLV would be **80:07:69:6F:73:2E:63:66:67**, where **80** is the suboption type (128 decimal), **07** is the length of the data, and the data is the filename expressed in hexadecimal ASCII values.

The complete **hex** data string would be **08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67**. The complete command would be **option 43 hex 08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67**.

Note When using the **option 43** command, you must manually calculate the length value for each TLV that you specify in the **hex** data string. However, you do not have to calculate the length for entire **option 43** command, because that is calculated automatically by the CMTS.

Caution Be certain that you have correctly entered the TLV data when using the **hex** option. Incorrectly entered data could cause CMs to reset, go offline, or hang, requiring a power cycle before being able to continue.

The following example shows how to specify a static downstream frequency for a Cisco uBR905, Cisco uBR924, Cisco uBR925, or Cisco CVA, using the **option 43** command to specify Cisco vendor-specific option 1.

```
router(config)# cable config-file statfreq.cm
router(config-file)# option 43 hex 08:03:00:00:0C:01:04:05:7F:9F:90
router(config-file)# exit
router(config)#
```

The hexadecimal data shown in this command consists of the two TLVs shown in Table 0-31:

Table 0-31 TLV Values for Sample Option 43 Command

Type	Length	Value
TLV 1—Vendor ID, Suboption 8		
08	03	00:00:0C (the ID for Cisco cable equipment)
TLV2—Static Downstream Frequency, Suboption 1		
1	04	05:7F:9F:90 (sets the downstream for the static frequency of 92,250,000 Hz)

Note Both the Cisco vendor-specific option for a static downstream frequency and the frequency **command** instruct the CM to move to a specific downstream frequency, overriding the frequency the CM found during its initial downstream scanning. However, the vendor-specific option requires the CM to use the specified frequency—if the CM loses its lock on that frequency or can never lock on to that specific frequency, the CM cannot go online. In contrast, the **frequency** command allows the CM to scan the downstream for the next available frequency if the CM loses its lock on the originally specified frequency.

The following example shows how to configure a Cisco uBR924, Cisco uBR925, or Cisco CVA122 so that it downloads a Cisco IOS configuration file named **ios.cfg** and configures the router for two voice ports. Three vendor-specific options are included: suboption 8, which specifies the vendor ID, suboption 128, which specifies the configuration file name, and suboption 10, which specifies the number of active voice ports.

```
router(config)# cable config-file iosfile.cm
router(config-file)# option 43 hex 08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67:0A:01:02
router(config-file)# exit
router(config)#
```

The hexadecimal data shown in this command consists of the three TLVs shown in Table 0-32:

Table 0-32 TLV Values for Sample Option 43 Command

Type	Length	Value
TLV 1—Vendor ID, Suboption 8		
08	03	00:00:0C (the ID for Cisco cable equipment)
TLV2—Cisco IOS Configuration File, Suboption 128		
80	07	69:6F:73:2E:63:66:67 (ASCII hexadecimal bytes for **ios.cfg**)
TLV3—Number of Active Voice Ports, Suboption 10		
0A	1	02 (two voice ports)

Cisco CMs also support giving a limited number of Cisco IOS configuration mode commands in the DOCSIS configuration file, using vendor-specific suboption 131. The following example shows how to use the **option 43** command to specify that the Cisco CM should execute the **ip http cable-monitor advance** command to enable its onboard Cable Monitor web server.

```
router(config-file)# option 43 hex 08:03:00:00:0C:83:1D:69:70:20:68:74:74:70:20:63:61:62:
6C:65:2D:6D:6F:6E:69:74:6F:72:20:61:64:76:61:6E:63:65
router(config-file)#
```

Table 0-33 lists the two TLVs shown in this example:

Table 0-33 TLV Values to Enable the Cisco Cable Monitor

Type	Length	Value
TLV 1—Vendor ID, Suboption 8		
08	03	00:00:0C (the ID for Cisco cable equipment)
TLV2—Cisco IOS Command, Suboption 131		
83	1D	69:70:20:68:74:74:70:20:63:61:62:6C:65:2D:6D:6F:6E:69:74:6F:72:20:61:64:76:61:6E:63:65 (ASCII hexadecimal bytes for **ip http cable-monitor advance**)

The following example shows the **instance** keyword being used to give multiple **option 43** commands. This example uses the same commands shown in the previous three examples.

```
router(config-file)# option 43 instance 1 hex 08:03:00:00:0C:01:04:05:7F:9F:90
router(config-file)# option 43 instance 2 hex 08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67:
0A:01:02
router(config-file)# option 43 instance 3 hex
08:03:00:00:0C:83:1D:69:70:20:68:74:74:70:20:63:61:62:6C:65:2D:6D:6F:6E:69:74:6F:72:20:61:
64:76:61:6E:63:65
```

```
router(config-file)#
```

The following example shows an attempt to specify two options that cannot be specified through the DOCSIS configuration file. Option 12 is reserved for the DOCSIS registration process, and Option 9 must be specified using the **download** command.

```
router(config-file)# option 12 ip 10.11.12.13
%Option 12 must not be specified manually
router(config-file)# option 9 ascii newsoftware.file
%Option 9 must be specified directly (not as raw option)
router(config-file)#
```

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.
privacy	Specifies privacy options for baseline privacy images.
service-class	Specifies service class definitions for the configuration file.
snmp manager	Specifies Simple Network Management Protocol (SNMP) options.
timestamp	Enables time-stamp generation.

packetcable

To enable PacketCable operations on the Cisco CMTS, use the **packetcable** command in global configuration mode. To disable PacketCable operations, use the **no** form of this command.

packetcable

no packetcable

Syntax Description

This command has no keywords or arguments.

Command Default

PacketCable operation is disabled.

Command Modes

Global Configuration

Command History

Release	Modification
12.2(8)BC2	This command was introduced for the Cisco uBR7200 series universal broadband router.
12.2(11)BC1	Support was added for automatically creating a random Element ID when PacketCable operations are enabled.
12.2(15)BC1	Support was added for the Cisco uBR10012 router.

Usage Guidelines

This command enables PacketCable operations on all cable interfaces and takes effect immediately. If you do not need to change any parameters from their default values, this is the only command needed to enable PacketCable operations.

In Cisco IOS Release 12.2(11)BC1 and later releases, this command also automatically creates a random Element ID for the CMTS that is in the range of 0 and 99,999. To ensure that this Element ID is unique across the entire PacketCable domain, you should use the **packetcable element-id** command.

Note PacketCable operations can be configured together with HCCP N+1 redundancy, but the PacketCable states are not synchronized between the Working and Protect interfaces. If a switchover occurs, existing voice calls continue, but when the user hangs up, PacketCable event messages are not generated because the Protect interface is not aware of the previous call states. However, new voice calls can be made and proceed in the normal fashion.

Channel Width Limitations

The 200,000 Hz channel width cannot be used on upstreams that support PacketCable voice calls, or on any upstreams that use Unsolicited Grant Service (UGS) or UGS with Activity Detection (UGS-AD) service flows. Using this small a channel width with voice and other UGS/UGS-AD service flows results in calls being rejected because of “DSA MULTIPLE ERRORS”.

Examples

The following example shows PacketCable operation being enabled:

```
Router# configure terminal
Router(config)# packetcable
Router(config)#
```

The following example shows PacketCable operation being disabled (default):

```
Router# configure terminal
Router(config)# no packetcable
Router(config)#
```

Related Commands

Command	Description
clear packetcable gate counter commit	Resets the counters that track the total number of committed gates.
packetcable authorize vanilla-docsis-mta	Allows Unsolicited Grant Service (UGS) service flows without a proper PacketCable gate ID when PacketCable operations are enabled on the Cisco CMTS.
packetcable element-id	Configures the PacketCable Event Message Element ID.
packetcable gate maxcount	Changes the maximum number of PacketCable gate IDs in the gate database on the Cisco CMTS.
packetcable timer	Changes the value of the different PacketCable DQoS timers.
show packetcable gate	Displays information about one or more gates in the gate database.
show packetcable gate counter commit	Displays the total number of committed gates since system reset or since the counter was last cleared.
show packetcable global	Displays the current PacketCable configuration.

packetcable authorize vanilla-docsis-mta

To allow Unsolicited Grant Service (UGS) service flows without a proper PacketCable gate ID when PacketCable operations are enabled on the Cisco CMTS, use the **packetcable authorize vanilla-docsis-mta** command in global configuration mode. To prevent CMs from requesting non-PacketCable UGS service flows when PacketCable operations are enabled, use the **no** form of this command.

packetcable authorize vanilla-docsis-mta

no packetcable authorize vanilla-docsis-mta

Syntax Description

This command has no keywords or arguments.

Command Default

Non-PacketCable UGS service flows are not allowed when PacketCable operations are enabled.

Command Modes

Global Configuration

Command History

Release	Modification
12.2(11)BC2	This command was introduced for the Cisco uBR7200 series universal broadband router.
12.2(15)BC1	Support was added for the Cisco uBR10012 router.

Usage Guidelines

By default, when PacketCable operations are enabled (using the **packetcable** ccommand), CMs must follow the PacketCable protocol when requesting UGS service flows. This prevents DOCSIS CMs that do not support PacketCable operations from using DOCSIS-style UGS service flows.

If you have a mixed network that contains both PacketCable and non-PacketCable DOCSIS CMs, you can allow DOCSIS CMs to request UGS service flows by using the **packetcable authorize vanilla-docsis-mta** command. If, however, your CMTS is providing PacketCable services, use the **no packetcable authorize vanilla-docsis-mta** command to disable DOCSIS-style service flows. This is the default configuration when PacketCable operations are enabled, and it requires that CMs must provide a validly authorized gate ID before being granted a UGS service flow.

Examples

The following example shows PacketCable operation being enabled, while still allowing DOCSIS-style UGS service flows:

```
Router# configure terminal
Router(config)# packetcable
Router(config)# packetcable authorize vanilla-docsis-mta
Router(config)#
```

The **show packetcable global** command has also been enhanced to display whether non-PacketCable DOCSIS-style UGS service flows are allowed:

```
Router# show packetcable global
```

```
Packet Cable Global configuration:
Enabled   : Yes
Element ID: 12456
Max Gates : 1048576
Allow non-PacketCable UGS
Default Timer value -
  T0      : 30000 msec
  T1      : 300000 msec
  T2      : 2000 msec
  T5      : 500 msec
Router#
```

Related Commands

Command	Description
clear packetcable gate counter commit	Resets the counters that track the total number of committed gates.
packetcable	Enables PacketCable operations on the Cisco CMTS.
packetcable element-id	Configures the PacketCable Event Message Element ID.
packetcable gate maxcount	Changes the maximum number of PacketCable gate IDs in the gate database on the Cisco CMTS.
packetcable timer	Changes the value of the different PacketCable DQoS timers.
show packetcable gate	Displays information about one or more gates in the gate database.
show packetcable gate counter commit	Displays the total number of committed gates since system reset or since the counter was last cleared.
show packetcable global	Displays the current PacketCable configuration.

packetcable element-id

To configure the PacketCable Event Message Element ID on the Cisco CMTS, use the **packetcable element-id** command in global configuration mode. To reset the counter to its default value, use the **no** form of this command.

packetcable element-id *n*

no packetcable element-id

Syntax Description

n	PacketCable Event Message Element ID for the Cisco CMTS. The valid range is 0 through 99999, with a default that is a random number in that range.

Command Default

A random value between 0 and 99,999.

Command Modes

Global Configuration

Command History

Release	Modification
12.2(11)BC1	This command was introduced for the Cisco uBR7200 series universal broadband router.
12.2(15)BC1	Support was added for the Cisco uBR10012 router.

Usage Guidelines

The PacketCable Event Message specification (PKT-SP-EM-I03-011221) requires that each trusted PacketCable network element that generates an Event Message MUST identify itself with a static Element ID that is unique across an entire PacketCable domain. This command allows you to configure the CMTS with an Element ID that is unique for your particular network. If you do not manually configure this parameter with the **packetcable element-id** command, it defaults to a random value between 0 and 99,999 when PacketCable operations is enabled.

The CMTS includes the Element ID in its Event Messages, along with its timezone information. You can display the current value using the **show packetcable global** command.

Examples

The following example shows the Event Message Element ID for this particular CMTS being set to 12456:

```
Router# configure terminal
Router(config)# packetcable element-id 12456
Pktcbl: Configured element ID 12456
Router(config)#
```

Related Commands

Command	Description
packetcable	Enables PacketCable operations on the Cisco CMTS.
packetcable authorize vanilla-docsis-mta	Allows Unsolicited Grant Service (UGS) service flows without a proper PacketCable gate ID when PacketCable operations are enabled on the Cisco CMTS.
packetcable gate maxcount	Changes the maximum number of PacketCable gate IDs in the gate database on the Cisco CMTS.
packetcable timer	Changes the value of the different PacketCable DQoS timers.
show packetcable global	Displays the current PacketCable configuration, including the Element ID.

packetcable gate maxcount

To change the maximum number of PacketCable gate IDs in the gate database on the Cisco CMTS, use the **packetcable gate maxcount** command in global configuration mode. To reset the counter to its default value, use the **no** form of this command.

packetcable gate maxcount *n*

no packetcable gate maxcount

Syntax Description

n	Maximum number of gate IDs to be allocated in the gate database on the CMTS. The valid range is 512 through 2097152, with a default value of 2097152 (8 * 512 * 512), which is sufficient to support 8 cable interface line cards.

Command Default

2097152 gate IDs

Command Modes

Global Configuration

Command History

Release	Modification
12.2(8)BC2	This command was introduced for the Cisco uBR7200 series universal broadband router.
12.2(11)BC2	The maximum number of possible gates and the default number of gates were doubled from 1,048,576 to 2,097,152 to accommodate a maximum of eight cable interface line cards (where each cable interface line card can use a maximum of 512*512, or 262,144, gates).
12.2(15)BC1	Support was added for the Cisco uBR10012 router.

Usage Guidelines

This command configures the number of gate IDs that the Cisco CMTS can store in its gate database. Because each PacketCable gate ID typically refers to both an upstream gate and a downstream gate, multiple this number by 2 to get the maximum number of gates that can be created on the CMTS.

Note Each cable interface line card supports a maximum of 512*512 (262,144) PacketCable gates, so ensure that you set the maximum number of gates to accommodate all installed cable interface line cards.

Examples

The following example shows the maximum number of gate IDs being set to 524288, which is sufficient for two cable interface line cards:

```
Router# configure terminal
Router(config)# packetcable gate maxcount 524288
Router(config)#
```

Related Commands

Command	Description
packetcable	Enables PacketCable operations on the Cisco CMTS.
packetcable authorize vanilla-docsis-mta	Allows Unsolicited Grant Service (UGS) service flows without a proper PacketCable gate ID when PacketCable operations are enabled on the Cisco CMTS.
packetcable element-id	Configures the PacketCable Event Message Element ID.
packetcable timer	Changes the value of the different PacketCable DQoS timers.
show packetcable global	Displays the current PacketCable configuration.

packetcable gate send-subscriberID

To include subscriber identification in GATE-OPEN and GATE-CLOSE gate control messages, use the **packetcable gate send-subscriberID** command in global configuration mode. To remove subscriber identification information from the gate control messages, use the **no** form of this command.

packetcable gate send-subscriberID

no packetcable gate send-subscriberID

Syntax Description

This command has no arguments or keywords.

Command Default

No subscriber identification information is provided in the GATE-OPEN and GATE-CLOSE gate control messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(23)BC1	This command was introduced.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB. Support for the Cisco uBR7225VXR router was added.

Examples

The following example enables gate control subscriber identification information using the **packetcable gate send-subscriberID** command:

```
Router(config)# packetcable gate send-subscriberID
```

Related Commands

Command	Description
packetcable	Enables PacketCable operation.
show packetcable gate	Displays information about one or more gates in the gate database.
show packetcable global	Displays the current PacketCable configuration.

packetcable timer

To change the value of the different PacketCable Dynamic Quality of Service (DQoS) timers, use the **packetcable timer** command in global configuration mode. To reset a timer to its default value, use the **no** form of this command.

packetcable timer {**T0** *timer-value* | **T1** *timer-value* | **multimedia T1** *timer-value*}

no packetcable timer {**T0** *timer-value* | **T1** *timer-value* | **multimedia T1** *timer-value*}

Syntax Description

T0 *timer-value*	Sets the T0 timer in milliseconds. The valid range is from 1 to 1,000,000,000 milliseconds, with a default value of 30000 milliseconds (30 seconds).
T1 *timer-value*	Sets the T1 timer in milliseconds. The valid range is from1 to 1,000,000,000 milliseconds, with a default value of 200000 milliseconds (200 seconds).
multimedia T1 *timer-value*	Sets the PacketCable multimedia T1 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 200000 milliseconds (200 seconds).

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
12.2(8)BC2	This command was introduced for the Cisco uBR7200 series universal broadband router.
12.2(11)BC2	The T2 and T5 timers were removed to conform to the requirements of the PacketCable DQoS Engineering Change Notice (ECN) 02148.
12.2(15)BC1	Support was added for the Cisco uBR10012 router.

Usage Guidelines

This command sets the following timers, which are defined in the *PacketCable™ Dynamic Quality-of-Service Specification* (PKT-SP-DQOS-I03-020116):

- T0 specifies the amount of time that a gate ID can remain allocated without any specified gate parameters. The timer begins counting when a gate is allocated with a Gate-Alloc command. The timer stops when a Gate-Set command marks the gate as Authorized. If the timer expires without a Gate-Set command being received, the gate is deleted.
- T1 specifies the amount of time that an authorization for a gate can remain valid. It begins counting when the CMTS creates a gate with a Gate-Set command and puts the gate in the Authorized state. The timer stops when the gate is put into the committed state. If the timer expires without the gate being committed, the CMTS must close the gate and release all associated resources.

Note The new timer values apply to all gates that are created after giving the command. Existing gates are not affected.

Examples

The following example shows the T0 timer being set to 20 seconds (20,000 milliseconds):

```
Router# configure terminal
Router(config)# packetcable timer T0 20000
Router(config)#
```

Related Commands

Command	Description
packetcable	Enables PacketCable operations on the Cisco CMTS.
packetcable authorize vanilla-docsis-mta	Allows Unsolicited Grant Service (UGS) service flows without a proper PacketCable gate ID when PacketCable operations are enabled on the Cisco CMTS.
packetcable element-id	Configures the PacketCable Event Message Element ID.
packetcable gate maxcount	Changes the maximum number of PacketCable gate IDs in the gate database on the Cisco CMTS.
show packetcable global	Displays the current PacketCable configuration.show packetcable global

peak-time1

To specify peak and offpeak monitoring times on a Cisco CMTS router, use the **peak-time1** command in enforce-rule configuration mode. To disable configuration of peak monitoring times, use the **no** form of this command.

peak-time1 {*hour*| *hour:minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate*] [**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes* [**penalty** *minutes*] {**downstream** | **upstream**}[**enforce**]

no peak-time1 {*hour*| *hour:minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** {*hour*| *hour:minutes*} **duration** *minutes* **avg-rate** *rate*] [**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes* [**penalty** *minutes*] {**downstream** | **upstream**}[**enforce**]

Syntax Description

hour | *hour:minutes*	Specifies the time of day, in either hh or hh:mm format, during which monitoring occurs for the peak time. If the time is specified in hour (hh), the valid range is 1 to 23 using a 24-hour clock. If the time is specified in hour:minutes (hh:mm), the valid range for hour is 1 to 23 using a 24-hour clock, and the valid range for minutes is 0 to 59.
duration *minutes*	Specifies the size of the sliding window (in minutes) during which the subscriber usage is monitored for the first peak time, and optionally for a second peak time when used with the **peak-time2** keyword. The valid range is 60 to 1440.
avg-rate *rate*	Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 kilobits with no default.
duration *offpeak-minutes*	(Optional) Specifies the size of the sliding window (in minutes) during which the subscriber usage is monitored for the remaining offpeak time (time not specified for peak monitoring). The valid range is 60 to 1440.
avg-rate *offpeak-rate*	Specifies the average sampling rate in kilobits per second for the specified offpeak duration. The valid range is 1 to 400000 kilobits with no default.
peak-time2 *hour* | *hour:minutes*	(Optional) Specifies the time of day during which monitoring occurs for a second peak time. The time can be specified either in hour or hour:minutes format. The valid range for hour is 1 to 23 using a 24-hour clock, and the valid range for minutes is 0 to 59.
sample-interval *minutes*	Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30, with a default value of 15.
penalty *minutes*	(Optional) Specifies the period (in minutes) during which a cable modem can be under penalty. The valid range is 1 to 10080.
downstream	Specifies monitoring of traffic in the downstream direction.
upstream	Specifies monitoring of traffic in the upstream direction.
enforce	(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.

Command Default

Peak and offpeak monitoring is disabled. The only default value for the **peak-time1** command is the 15-minute sample interval.

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.
12.2(33)SCD2	The minute-level granularity (hh:mm) for **peak-time1**and **peak-time2** duration, and the **penalty** keyword option were added.

Usage Guidelines

Note This command is applicable only after the **monitoring-basics** command is configured with the keyword **peak-offpeak**.

You can monitor two peak monitoring periods using the initial **peak-time1** command and its options, followed by the **peak-time2** keyword and the corresponding options. The remaining hours are considered offpeak and can be monitored by configuring the optional **duration** keyword and the corresponding options.

The **penalty** duration, which is configured using the **peak-time1** command, is unique to weekdays, and takes precedence over the global penalty duration configured using the **penalty-period** command.

When you use the **show running-configuration** command to display the configuration, the keyword options for the **peak-time1** command are truncated. In the following example, "d" represents **duration** (a single peak and offpeak duration are configured), "avg" represents **avg-rate**, "sa" represents **sample-interval**, "pen" represents **penalty**, "do" represents **downstream**, and "enf" represents **enforce**:

```
Router# show running-configuration
.
.
.
peak-time1 1 d 60 avg 2 d 60 avg 40 sa 10 pen 11 do enf
```

Examples

The following example shows an enforce-rule that defines two peak monitoring periods for upstream traffic:

```
Router(enforce-rule)# peak-time1 10:30 duration 120 avg-rate 10 peak-time2 23 duration 60
avg-rate 10 sample-interval 10 penalty 11 upstream enforce
```

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.
monitoring-basics	Specifies the type of monitoring for subscriber traffic management on a Cisco CMTS router.
penalty-period	Specifies the period during which an enforced quality of service (QoS) profile should be in force for subscribers who violate their registered QoS profile.
qos-profile enforced	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles. This command is applicable for DOCSIS 1.0 cable modems
qos-profile registered	Specifies the registered QoS profile that should be used for this enforce-rule. This command is applicable for DOCSIS 1.0 cable modems
service-class (enforce-rule)	Identifies a particular service class for cable modem monitoring in an enforce-rule. This command is applicable for DOCSIS 1.1 or later cable modems.
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.
weekend peak-time1	Configures peak and offpeak subscriber monitoring over weekends on a Cisco CMTS router.

penalty-period

To specify the time period that an enforced quality of service (QoS) profile should be in force for subscribers that violate their registered QoS profile, use the **penalty-period** command in enforce-rule configuration mode. To reset an enforce-rule to its default penalty period, use the **no** form of this command.

penalty-period *minutes* [**time-of-day** {*hour* | *hour:minutes*}] [**monitoring-on**]

no penalty-period

Syntax Description

minutes	Specifies a time period (in minutes) during which a cable modem (CM) can be under penalty. The range is 1 to 10080, with a default value of 10080 (7 days).
time-of-day {*hour* | *hour:minutes*}	(Optional) Specifies the time of day (in hh or hh:mm format) when: • A CM that is under penalty is released from the penalty period. • A CM that is not under penalty has its subscriber monitoring counters reset. If the time of day is specified in hour (hh), the valid range is 1 to 23 using a 24-hour clock. If the time of day is specified in hour:minutes (hh:mm), the valid range for hour is 1 to 23 using a 24-hour clock, and the valid range for minutes is 0 to 59.
monitoring-on	(Optional) Specifies that monitoring should be turned on after the penalty release time. If this keyword is not specified, by default, monitoring is turned off after the release time, until the end of the day, that is 00:00 hrs.

Command Default

The default time period is 10080 minutes (7 days).

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 integrated into Cisco IOS Release 12.3(9a)BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.3(23)BC2	The **time-of-day** keyword option was added.
12.3(23)SCD2	The minute-level granuality for the **time-of-day** duration, and the **monitoring-on** keyword option were added.

Usage Guidelines

When a subscriber overconsumes the maximum bandwidth that is specified in the enforce-rule, the Cisco CMTS router can automatically switch the subscriber to an enforced QoS profile for the time duration configured with the **penalty-period** command. When the penalty period expires, the Cisco CMTS router restores the subscriber to their registered QoS profile.

The penalty duration specified in the **penalty-period** command is a global configuration. This penalty duration is overridden if the individual penalty duration is already configured using the **duration**, **weekend duration**, **peaktime1** or **weekend peaktime1** commands. Similarly, if the individual penalty duration is not configured, the global penalty duration is used. Table 34 explains in detail the criteria for choosing the penalty duration:

Table 34 Criteria for Choosing Penalty Duration

Global Penalty-Period Configured	Weekday Penalty-Period Configuration (CLI: duration or peaktime1)	Weekend Penalty-Period Configuration (CLI: weekend duration, or weekend peaktime1)	Applied Penalty Duration for Weekdays	Applied Penalty Duration for Weekends
Yes	Yes	Yes	Weekday Penalty Configuration	Weekend Penalty Configuration
Yes	Yes	No	Weekday Penalty Configuration	Global Penalty Configuration
Yes	No	Yes	Global Penalty Configuration	Weekend Penalty Configuration
Yes	No	No	Global Penalty Configuration	Global Penalty Configuration

If the keyword **monitoring-on** is specified, monitoring starts immediately after the cable modems are released from penalty. However if this keyword is not specified, by default, all the cable modems using the enforce-rule are not monitored until the end of day, that is, 00:00 hrs.

The penalty period continues across reboots of the cable modem, so a user cannot avoid the enforced QoS profile by trying to reset their modem and reregister on the cable network. This allows service providers to set an appropriate penalty for users who consistently exceed the allocated maximum bandwidth.

Note To manually move a DOCSIS 1.0 cable modem back to its registered profile before the end of the penalty period, use the **cable modem qos profile** command. To manually move a DOCSIS 1.1(or later) cable modem back to its registered profile before the end of the penalty period, use the **cable modem {ip-address | mac-address} service-class-name** command.

When you change the configuration of a currently active enforce-rule, that rule begins using the new configuration immediately to manage the cable modems tracked by this enforce-rule.

Note Before making any changes to an active enforce-rule, we recommend that you first disable the enforce rule using the **no enabled** command.

A cable modem consists of two service flows, Primary upstream and Primary downstream. If a DOCSIS 1.0 cable modem enters the penalty period because one of its service flows has exceeded its allowed bandwidth, the QoS profile of the entire modem is changed. However, if a DOCSIS 1.1 or later cable modem enters the penalty period because its upstream or downstream service flow has exceeded the allowed bandwidth threshold, the service class name is changed only for the upstream or downstream service flow.

Examples

The following example shows an enforce-rule named "test", which is configured with a penalty period of 1440 minutes (1 day):

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# penalty-period 1440
```

The following example shows an enforce-rule named "test", which is configured with a penalty period of 1440 minutes (1 day), but allowing the removal of the cable modems in penalty at 23:00. Monitoring will be turned off by default at 23:00, to 00:00 (1 hour):

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# penalty-period 1440 time-of-day 23
```

The following example shows an enforce-rule named "test", which is configured with a penalty period of 1440 minutes (1 day), allowing the removal of the cable modems in penalty at 23:00. However, after the cable modems are released from penalty, fresh monitoring starts, with all the subscriber monitoring counters reset to 0:

```
Router# configure terminal
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# penalty-period 1440 time-of-day 23 monitoring-on
```

Related Commands

Command	Description
cable qos enforce-rule	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic monitoring, and enters the 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.
qos-profile enforced	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles. This command is applicable for only DOCSIS 1.0 cable modems.
qos-profile registered	Specifies the registered QoS profile that should be used for this enforce-rule. This command is applicable for only DOCSIS 1.0 cable modems.
service-class (enforce-rule)	Specifies a service class (enforced or registered) that should be used for the cable modem monitoring in an enforce-rule. This command is applicable for DOCSIS 1.1 or later cable modems.
show cable qos enforce-rule	Displays the QoS enforce-rules that are defined.
show cable subscriber-usage	Displays subscribers who are violating their registered QoS profiles.

periodic-rel-pxf enable

To enable the Reload PXF in the Standby PRE Support feature, use the **periodic-rel-pxf enable** command in redundancy configuration mode. To disable the Reload PXF in the Standby PRE feature, use the **no** form of this command.

periodic-rel-pxf enable

no periodic-rel-pxf enabled

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
12.2(33)SCG2	This command was introduced.

Usage Guidelines

The **periodic-rel-pxf enable** command is supported on Cisco uBR10012 router only.

Examples

The following example shows how to enable the Reload PXF on Standby PRE feature on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# periodic-rel-pxf enable
Router(config-red)# end
```

Associated Features

The **periodic-rel-pxf enable** command is used to enable the Reload PXF on Standby PRE Support feature.

ping docsis

To determine whether a specific cable modem (CM) is reachable from the CMTS at the DOCSIS MAC layer, use the **ping docsis** command in privileged EXEC mode.

ping docsis {*mac-addr* | *ip-addr* | **name** *fqdn*} [*count*] [**repeat** *queue-intervals*] [**verbose**]

Syntax Description

mac-addr	The 48-bit hardware (MAC) address of the CM. If you specify the MAC address of a CPE device, the command will resolve it to the MAC address of the CM servicing that CPE device and send the DOCSIS ping to the CM.
ip-addr	IPv4 or IPv6 address of the CM. If you specify the IP address of a CPE device, the command will resolve it to the IP address of the CM servicing that CPE device and send the DOCSIS ping to the CM.
name *fqdn*	Specifies the fully qualified domain name (FQDN) of the cable device to be displayed. This option is only available if the **show cable modem domain-name** command has been run for the first time to update the cable DNS cache on the CMTS router.
repeat *queue-intervals*	(Optional) Specifies the number of maintenance intervals for a queue. Valid values are from 1 to 2147483647.
verbose	(Optional) Specifies verbose mode for the output, giving additional details about the packets transmitted and received.

Command Default

If no count is specified, five DOCSIS ping packets are sent.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 NA	This command was introduced for the Cisco uBR7200 series router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.1(1a)T1	The command output was enhanced.
12.1(3)XQ1	Support was added for wireless radio modems.
12.1(5)EC	Support was added for the Cisco uBR7100 series routers.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(1)XF1	Support was added for the Cisco uBR10012 router.
12.2(4)BC1	This command was integrated into Cisco IOS Release 12.2(4)BC1.

Release	Modification
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA, with the following changes: • Support for the Cisco uBR7225VXR router was added. • Support for specifying the IPv6 address of a CM or CPE device was added. • The **name** keyword option was added for specifying the fully-qualified domain name of a CM.
12.2(33)SCC	The **repeat** keyword was added to specify maintenance intervals for queues.

Usage Guidelines

The DOCSIS ping is a unique Cisco patented technology that allows a cable operator to quickly diagnose the health of a channel between the CMTS router and any particular DOCSIS cable CPE device. The DOCSIS ping is similar in concept to the IP ping but uses the lower MAC layer instead of the datalink or transport layers. Using the MAC layer has two major advantages:

- A DOCSIS ping uses only 1/64 of the bandwidth of an IP ping.
- A DOCSIS ping can be used with CMs that have not yet acquired an IP address. This allows cable operators to ping CMs that were not able to complete registration or that were improperly configured at the IP layer.

In addition to providing connectivity information, the **ping docsis** command provides a real-time view and plot of requested power adjustments, frequency, timing offset adjustments, and a measure of optimal headend reception power.

If a CM responds to the **ping docsis** command, but does not respond to an IP ping, the problem could be one of the following:

- The CM is still in the registration process and has not yet come completely online. In particular, the CM could be waiting for the DHCP server to assign it an IP address.
- Severe interference or other faults on the physical layer (either the upstream or downstream).
- Significant upstream signal error, distortion, or amplitude errors, often resulting in frequent power adjustments (which are shown in the cable flap list).
- A non-DOCSIS compliant upstream carrier-to-noise power ratio (C/N) that is between 14 and 21 dB, along with a mixed modulation profile, such as ranging request/response messages being sent in QPSK mode and short and long data grants in 16-QAM mode.

Note The **ping docsis** command is a DOCSIS-compliant process that can be used with any two-way DOCSIS-compliant CM; the CM does not require any special features or code. The **ping docsis** command cannot be used with telco-return CMs.

Note In Cisco IOS Release 12.2(33)SCA, the **show cable modem domain-name** command must be run first on the route processor (RP) of the CMTS router before any domain name can be used as part of a cable command.

Table 35 explains the different characters that can appear in the output for the **ping docsis** command:

Table 35 ping docsis Command Output Characters

Output Character	Description
!	Indicates that a successful response was received from the ping request. This indicates that the CM is reachable from the CMTS and can respond to CMTS requests at the DOCSIS MAC layer.
.	Indicates that a DOCSIS ping request was sent out but that the ping request timed out without receiving a response. This indicates that the CM is having difficulties maintaining DOCSIS MAC layer connectivity to the CMTS. **Note** If the **ping docsis** command displays a number of periods (.) along with exclamation points (!), it strongly indicates the presence of RF noise or physical cable and plant issues that is causing a loss of MAC layer connectivity.
a	Indicates that a response was received but that an adjustment of frequency, power, or timing was also made in the response. This indicates that, although the upstream channel is functional, some sort of problem is forcing power averaging and other misreads of the upstream received power signals.
f	Indicates that the CMTS failed to send the DOCSIS ping request because the CM is offline, and therefore MAC-layer communication is not possible. This indicates that the CM had previously registered with the CMTS, but that at some point it stopped responding to the DOCSIS station maintenance messages and that the CMTS eventually marked the CM as offline. The CM might have lost power or might have been disconnected from the coaxial cable. **Tip** Use the **show cable modem** command with the same MAC or IP address as you used with the **ping docsis** command to show the current status of this CM.

Note If a CM is already in the flap list, the **ping docsis** command increments the hit, miss, and power-adjustment fields for it in the cable flap list.

Examples

The following example shows a default **ping docsis** command that sends five packets to the CM with the MAC address of 00d0.ba77.7595, with a response being received for each:

```
Router# ping docsis 00d0.ba77.7595

Queueing 5 MAC-layer station maintenance intervals, timeout is 25 msec:
!!!!!
Success rate is 100 percent (5/5)

Router#
```

The following example shows the verbose output for the same command:

```
Router# ping docsis 00d0.ba77.7595 verbose

Queueing 5 MAC-layer station maintenance intervals, timeout is 25 msec:
Reply from 00d0.ba77.7595: 2 ms, tadj=-1, padj=0.50, fadj=0
Reply from 00d0.ba77.7595: 2 ms, tadj=-1, padj=0.50, fadj=0
Reply from 00d0.ba77.7595: 2 ms, tadj=-1, padj=0.50, fadj=0
Reply from 00d0.ba77.7595: 98 ms, tadj=-1, padj=0.25, fadj=0
Reply from 00d0.ba77.7595: 2 ms, tadj=-1, padj=0.25, fadj=0

Success rate is 100 percent (5/5)

Router#
```

The following example shows that the CM at 192.168.100.10 is connected to the network and is operational, but that one ping packet was lost and that several power adjustments were made during the ping process:

```
router# ping docsis 192.168.100.10

Queueing 100 MAC-layer station maintenance intervals, timeout is 25 msec:
!!!!!a!!!!!!!a!a!!!!!!!!!!!!!!!!!!!!!!aa!!!!!!!!!!a!!!a!a!!!aa!!!!!!.!!a!!!a!
a!a!!!!!!!!aa!!!!!!!aa!a
Success rate is 99 percent (99/100)
```

A CM that displays output such as that above (a higher percentage of successful pings but with a number of power-adjustment readings) is most likely experiencing a problem that is not bad enough to force the modem offline but that should be addressed.

If this problem is consistent for just a small number of CMs on an upstream receiver (such as a fiber node within a combining group), then the problem is likely related to in-home wiring at those modem locations. It could also be due to a cable TV network element that is on the same HFC segment.

If the problem occurs for all CMs on a single fiber node, then changing the upstream frequency or reducing the number of homes passed per combining group might improve conditions. If this does not help the situation, the problem could be due to a faulty cable drop, dirty optical connector on the node, or other physical plant problem.

The **ping docsis** command cannot be used with a CM that has not yet registered with the CMTS. The following example shows the responses for a CM that has not yet registered with the CMTS.

```
router# ping docsis 192.168.100.111
Cable modem with IP address 192.168.100.111 not registered.
Please try using MAC address instead.

router# ping docsis 0123.4567.89ab
Cable modem with MAC address 0123.4567.89ab not registered.
router#
```

The following example shows the output of the **ping docsis** command with the **repeat** keyword:

```
router# ping docsis 192.168.100.10 repeat 22

Queueing 22 MAC-layer station maintenance intervals, timeout is 25 msec:
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (22/22)
```

Related Commands

Command	Description
cable flap-list aging	Specifies the number of days to keep a CM in the flap-list table before aging it out of the table.
cable flap-list insertion-time	Sets the insertion time interval that determines whether a CM is placed in the flap list.
cable flap-list miss-threshold	Specifies miss threshold for recording a flap-list event.
cable flap-list power-adjust threshold	Specifies the power-adjust threshold for recording a CM flap-list event.
cable flap-list size	Specifies the maximum number of CMs that can be listed in the flap-list table.
clear cable flap-list	Clears all the entries in the flap-list table.
ping	Outputs one or more IP ping requests to a particular IP address.
show cable flap-list	Displays the current contents of the flap list.

plim qos input map

To configure a priority queue on Gigabit Ethernet SPAs, use the **plim qos input map** command in interface or subinterface configuration mode. To remove a priority queue, use the no form of this command.

plim qos input map {cos {**enable** | *cos-value* **queue low-latency**} | **ip** {**dscp-based** | **dscp** *dscp-value* **queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value* **queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value* **queue low-latency**

Syntax Description

cos enable	Enables classification of ingress VLAN traffic according to the 802.1Q priority bits. **Note** This command can only be applied to VLAN interfaces.
cos *cos-value* **queue low-latency**	Classifies incoming VLAN traffic on a subinterface according to the 802.1Q priority bits and places the traffic into the appropriate queue. By default, traffic with 802.1Q priority bits set to 6 or 7 are placed in the high-priority queue and all other traffic is placed in the low-priority queue. *cos-value s*pecifies the IEEE 802.1Q/ISL CoS value from 0 to 7. **Note** When you configure a class of service (CoS) value on a QinQ subinterface, the CoS value applies to all QinQ subinterfaces with the same outer VLAN ID. **low-latency** specifies the high priority queue.
ip dscp-based	Enables the classification of incoming IP traffic according to the value of the DSCP bits. **Note** This command only applies to physical interfaces.
ip dscp *dscp-value* **queue low-latency**	Classifies incoming IP traffic according to the value of the DSCP bits and places the traffic into the appropriate queue. By default, IP traffic with the DSCP bits equal to EF will use the low-latency queue, and traffic with any other DSCP value will use the low-priority queue. *dscp-value* is the value of the DSCP bits. You can specify a range of values separated by a dash or a list of value. For a list of valid values, see the Usage Guidelines. **low-latency** specifies the high priority queue.
ip precedence-based	Enables the classification of incoming IP traffic according to the IP precedence value. **Note** This command applies only to physical interfaces.
ip precedence *precedence-value* **queue low-latency**	Classifies incoming IP traffic according to the value of the IP precedence bits and places the traffic into the appropriate queue. IP traffic with the IP precedence bits set to 6 or 7 uses the low-latency queue; all other traffic uses the low-priority queue. *precedence-value* is the value of the IP precedence bits (0 to 7). You can specify a range of values separated by a dash or a list of values. **low-latency** specifies the high priority queue.

ipv6 tc *tc-value* **queue low-latency**	Classifies ingress IPv6 traffic based on the value of the traffic-class bits and places the traffic into the appropriate queue. By default, IPv6 traffic with a traffic-class value equal to **ef** uses the high-priority queue and all other traffic uses the low-priority queue. Only the most significant six bits of the traffic-class octet is used for the classification. **Note** This command applies only to physical interfaces. *tc-value* is the value of the traffic class bits. You can specify a range of values separated by a dash or a list of values. For a list of valid values, see the Usage Guidelines. **low-latency** specifies the high priority queue.
mpls exp *exp-value* **queue low-latency**	Classifies incoming MPLS traffic according to the value of the EXP bits and places the traffic into the appropriate queue. By default, traffic with the EXP bits set to 6 or 7 uses the high-priority queue and all other traffic uses the low-priority queue. **Note** This command applies only to physical interfaces. *exp-value* is the value of the EXP bits (0 to 7). You can specify a range of values separated by a dash or a list of values. **low-latency** specifies the high priority queue.

Defaults

Disabled

Command Modes

Interface or subinterface configuration

Command History

Cisco IOS Release	Modification
12.2(33)SB	This command was introduced on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **plim qos input map** command separates high-priority traffic from low-priority traffic and places the traffic in the appropriate interface queue. The command separates priority and non-priority traffic at the SPA interface processor (SIP) to prevent the dropping of high priority traffic in an oversubscription case. Each shared port adaptor (SPA) supports one priority queue.

The router supports the following classification types for the prioritization of ingress traffic on the Gigabit Ethernet SPAs:

- VLAN 802.1Q priority bits
- IP DSCP bits
- IP precedence bits
- IPv6 traffic class bits
- MPLS experimental (EXP) bits

For the **plim qos input map ip dscp** *dscp-value* **queue low-latency** command, valid values for *dscp-value* are one of the following:

- 0 to 63—Differentiated services codepoint value
- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110
- af41—100010
- af42—100100
- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

For the **plim qos input map ipv6 tc** *tc-value* **queue low-latency** command, valid values for *tc-value* are one of the following:

- 0 to 63—Differentiated services codepoint value
- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110
- af41—100010
- af42—100100

- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

Examples

The following example enables DSCP-based classification on the SPA that is located in subslot 0 of the SIP in slot 1 of the Cisco 10000 series router:

```
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# plim qos input map ip dscp-based
```

Related Commands

Command	Description
card	Preprovisions the SIP-600 and SPAs.
negotiation auto	Enables autonegotiation on a Gigabit Ethernet SPA interfaces on the Cisco 10000 SIP-600.
mtu	Configures the maximum packet size for an interface. The default is 1500 bytes. The maximum configurable MTU is 9129 bytes.

policy

To select modems based on the type of service flow that is balanced, use the **policy** command in the config-lb-group configuration mode. To reset the selection, use the **no** form of this command.

policy {**pcmm | ugs | us-across-ds | pure-ds-load**}

no policy {**pcmm | ugs | us-across-ds | pure-ds-load**}

Syntax Description

pcmm	Enables balancing of modems with active PCMM service flows.
ugs	Enables balancing of modems with active UGS service flows.
us-across-ds	Sets load balancing on upstream (US) groups across downstream (DS) and DS group methods are ignored.
pure-ds-load	Considers DS load and not US load when calculating DS utilization.

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.

Examples

The following example shows how to select the modems on the CMTS based on the type of service flow that is balanced using the **policy** 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)# policy pure-ds-load
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.

prefix

To configure an IPv4 or IPv6 prefix in a source address verification (SAV) group, use the **prefix** command in SAV configuration mode. To disable the use of a configured prefix in a SAV group, use the **no** form of this command.

prefix {*ipv4_prefix/ipv4_prefix_length* | *ipv6_prefix/ipv6_prefix_length*}

no prefix {*ipv4_prefix/ipv4_prefix_length* | *ipv6_prefix/ipv6_prefix_length*}

Syntax Description

ipv4_prefix	IPv4 prefix associated with a particular SAV group, specified in the X.X.X.X/X format.
ipv4_prefix_length	Length of the IPv4 prefix. The valid range is from 0 to 32.
ipv6_prefix	IPv6 prefix associated with a particular SAV group, specified in the X:X:X:X::/X format.
ipv6_prefix_length	Length of the IPv6 prefix. The valid range is from 0 to 128.

Command Default

None

Command Modes

SAV Configuration (config-sav)

Command History

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

Usage Guidelines

The **prefix** command is used to configure IPv4 or IPv6 prefixes within a particular SAV groups. The Cisco CMTS uses these prefixes to authenticate a cable modem (CM). A CM may be configured with an IPv4 or IPv6 prefix belonging to a particular SAV group. The time, length, value (TLV) 43.7.2 specifies the prefix associated with the CM. The Cisco CMTS considers a packet from a CM authorized if that packet is sourced with an IP address that belongs to the configured prefix in a SAV group.

A maximum of four prefixes are supported on one SAV group. These prefixes can be either IPv4s, IPv6s, or a combination of both prefixes (maximum up to four)

Examples

The following example shows how to configure a SAV group with one IPv4 prefixes and one IPv6 prefixes:

```
Router(config)# cable source-verify group sav1
Router(config)# prefix 10.16.0.0/12
Router(config)# prefix 10::/12
Router(config)# exit
```

Command	Description
cable source-verify enable-sav-static	Enables SAV prefix processing.
cable source-verify group	Configures SAV groups.

profile-description

To provide a profile description for each profile in the selected cable multicast authorization profile, use the **profile-description** command in multicast authorization profile configuration mode. To remove the profile description, use the **no** form of this command.

profile-description *profile-description*

no profile-description *profile-description*

Syntax Description

profile-description	Specifies profile description for the selected profile. You can use up to 128 characters to describe the profile.

Command Default

Profile description is empty.

Command Modes

Multicast authorization configuration—(config-mauth)

Command History

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

Usage Guidelines

This command is available only from the cable multicast authorization profile mode.

Examples

The following example shows how to enter a profile description for a multicast authorization profile name:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable multicast auth profile-name
Router(config)# cable multicast auth profile-name gold
Router(config-mauth)# profile-description gold-configured-may
```

Related Commands

Command	Description
cable multicast authorization enable default-action	Enables the cable multicast authorization features.
cable multicast authorization profile-name	Defines the cable multicast authorization profile.

Command	Description
show cable multicast authorization	Displays the list of defined multicast authorization profiles and all CMs associated with corresponding profiles.
show running-config interface cable	Displays the running configuration for each of the cable interfaces.

protect-tunnel

To configure a Downstream External PHY Interface (DEPI) tunnel for the protect cable interface line card on a Cisco CMTS router, use the **protect-tunnel** command in global configuration mode. To disable this configuration, use the **no** form of this command.

protect-tunnel *protect-depi-tunnel-name*

no protect-tunnel *protect-depi-tunnel-name*

Syntax Description

protect-tunnel-name	DEPI tunnel name for the protect cable interface line card.

Command Default

The N+1 DEPI redundancy feature is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The protect tunnel must be explicitly configured. The working tunnel and the protect tunnel are configured using the same **depi-tunnel** command. The protect tunnel inherits L2TP class and DEPI class parameters from the working tunnel. When you configure the protect tunnel and specify the destination IP address for the protect tunnel, the protect tunnel inherits the QAM channel parameters specified for the working tunnel.

Examples

The following example shows how to configure a DEPI tunnel for the protect cable interface line card on the Cisco uBR10012 router:

```
Router> enable
Router# configure terminal
Router(config)# depi-tunnel protect1
Router(config-depi-tunnel)# dest-ip 192.0.2.103
Router(config-depi-tunnel)# exit
Router(config)# depi-tunnel depi-tunnel working1
Router(config-depi-tunnel)# protect-tunnel protect1
Router(config-depi-tunnel)# end
```

Related Commands

Command	Description
depi-tunnel	Specifies a template for DEPI tunnel configuration settings.

privacy

To create a DOCSIS configuration file that enables and configures the DOCSIS Baseline Privacy Interface (BPI) option, use the **privacy** command in cable config-file configuration mode. To disable BPI for the CM, use the **no** form of this command.

privacy grace-time {**authorization** *value* | **tek** *value*}

privacy timeout {**authorize** *value*| **operational** *value*| **re-authorize** *value*| **reject** *value*| **rekey** *value*}

no privacy grace-time {**authorization | tek**}

no privacy timeout {**authorize | operate | re-authorize | reject | rekey**}

Syntax Description

authorization *value*	Authorization grace time in seconds. Valid values are 1 to 1800 seconds. Default value is 600 seconds.
tek *value*	TEK grace time in seconds. Valid range is 1 to 1800 seconds. Default is 600 seconds.
authorize *value*	Authorize wait timeout in seconds. Valid range is 1 to 30 seconds. Default value is 10 seconds.
operational *value*	Operational Wait timeout in seconds. Valid range is 1 to 10 seconds. Default is 1 second.
re-authorize *value*	Re-authorize wait timeout in seconds. Valid range is 1 to 20 seconds.
reject *value*	Authorize reject wait timeout in seconds. Valid range is 1 to 600 seconds. Default is 60 seconds.
rekey *value*	Rekey wait timeout in seconds. Valid range is 1 to 10 seconds. Default is 1 second.

Command Default

No default behaviors or values

Command Modes

Cable config-file configuration

Command History

Release	Modification
12.1(2)EC1	This command was introduced.
12.2(11)BC2	This command was supported on the Release 12.2 BC train.

Usage Guidelines

Specifying the **privacy** command without any of the keywords and arguments enables BPI encryption and decryption for the CM. In addition to this command, you must also specify the **service-class privacy** command to enable BPI operations on the cable modem.

Note The **privacy** command appears and is supported only in images with support for BPI or BPI+ encryption. This option configures the CM for BPI or BPI+ encryption. To use BPI encryption, the Cisco CMTS must also be configured for BPI or BPI+ encryption, using the **cable privacy** command.

Examples

The following example shows how to set the CM privacy TEK gracetime to 1200 seconds and enables BPI operations for the cable modem.

```
router(config)# cable config-file bpi.cm
router(config-file)# privacy grace-time tek 1200
router(config-file)# service-class 1 privacy
router(config-file)# exit
router(config)#
```

Related Commands

Command	Description
access-denied	Disables access to the network.
cable config-file	Creates a DOCSIS configuration file and enters configuration file mode.
cable privacy	Enables BPI or BPI+ encryption on the Cisco CMTS.
channel-id	Specifies upstream channel ID.
cpe max	Specifies CPE information.
download	Specifies download information for the configuration file.
frequency	Specifies downstream frequency.
option	Provides config-file options.
service-class	Specifies service class definitions for the configuration file.
snmp manager	Specifies Simple Network Management Protocol (SNMP) options.
timestamp	Enables time-stamp generation.