



Cable Commands: cable o through cable r

- [cable ofdm-rf-change-trigger](#), page 4
- [cable ofdma-frequency-exclusion-band](#) , page 5
- [cable ofdma-frequency-unused-band](#), page 6
- [cable power](#), page 7
- [cable pre-equalization exclude](#), page 10
- [cable primary-sflow-qos11 keep](#), page 13
- [cable privacy](#), page 15
- [cable privacy bpi-plus-enforce](#), page 19
- [cable privacy bpi-plus-exclude](#), page 21
- [cable privacy bpi-plus-policy](#), page 23
- [cable privacy clone-detect](#), page 25
- [cable privacy eae-exclude](#), page 27
- [cable privacy eae-policy](#), page 29
- [cable privacy encrypt-alg-priority](#), page 31
- [cable privacy hotlist](#), page 33
- [cable privacy kek](#), page 36
- [cable privacy non-mtc-aes128](#), page 38
- [cable privacy revocation crl skip-sig-check](#), page 39
- [cable privacy revocation enable](#), page 41
- [cable privacy revocation oosp skip-sig-check](#), page 43
- [cable privacy revocation skip-cm-cert](#), page 45
- [cable privacy revocation timeout](#), page 47
- [cable privacy tek](#), page 49
- [cable profile](#), page 51

- [cable profile rpd-event](#), page 54
- [cable proxy-arp](#), page 56
- [cable qos enforce-rule](#), page 58
- [cable qos permission](#), page 62
- [cable qos pre-registration](#), page 65
- [cable qos pro max-ds-burst](#), page 67
- [cable queue-limit](#), page 70
- [cable rate-limit-algorithm min-plus-excess](#), page 72
- [cable rcc-template](#), page 74
- [cable rcc-templates frequency-based](#) , page 76
- [cable rcp-control](#), page 78
- [cable rcp-id](#), page 80
- [cable reduction-mode energy-management dynamic-channel-percent](#), page 82
- [cable reduction-mode energy-management enable](#), page 83
- [cable reduction-mode energy-management process-queue-size](#), page 84
- [cable reduction-mode energy-management ranging-init-technique](#), page 85
- [cable reduction-mode mta-battery](#) , page 86
- [cable redundancy hashfilter](#), page 88
- [cable redundancy myid](#), page 90
- [cable redundancy node](#), page 92
- [cable redundancy node frequency](#), page 94
- [cable redundancy target](#), page 96
- [cable redundancy threshold](#), page 98
- [cable registration-timeout](#), page 100
- [cable relay-agent-option](#), page 101
- [cable resiliency ds-bonding](#), page 103
- [cable resiliency traps-interval](#), page 104
- [cable rf-adapt timer](#), page 106
- [cable rf-bandwidth-percent](#), page 108
- [cable rf-change-dampen-time](#), page 111
- [cable rf-change-trigger](#), page 113
- [cable rf-channel](#), page 115
- [cable rf-channels](#) , page 120

- [cable rswitch copy](#), page 122
- [cable rswitch delete](#), page 124
- [cable rswitch reboot](#), page 126
- [cable rswitch set-active](#), page 127
- [cable rpd](#), page 128
- [cable rsvp default-scen](#), page 130

cable ofdm-rf-change-trigger

To configure the trigger thresholds specific to OFDM RF impairment, use the **cable ofdm-rf-change-trigger** command in global configuration mode. If this command is not configured, then the value configured in the **cable rf-change-trigger** command will apply.

cable ofdm-rf-change-trigger {*percent value* | *count number*}

Syntax Description

percent <i>value</i>	Indicates the percentage of cable modems that must report that a particular non-primary OFDM RF channel is down before that channel is suspended from the bonding group. The valid range is 1 to 100. The default is 0.
count <i>number</i>	Specifies the number of cable modems that must report that a particular non-primary OFDM RF downstream channel is down before that channel is suspended from the downstream bonding groups. The default is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Related Commands

Command	Description
cable rf-change-trigger	Specifies the amount of time an event must persist before it triggers an action for the reporting cable modem.

cable ofdma-frequency-exclusion-band

To exclude the range of frequencies from all OFDMA channels on a port, use the **cable ofdma-frequency-exclusion-band** command in controller configuration mode.

cable ofdma-frequency-exclusion-band *start value end value*

Syntax Description

<i>start value</i>	Specify the start value of the frequency range.
<i>end value</i>	Specify the end value of the frequency range.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Exclusion bands apply to OFDMA channels only. OFDMA channel does not use frequencies in exclusion band set by the **cable ofdma-frequency-exclusion-band** command. So the legacy SC-QAM channel can be placed in this band.

Related Commands

Command	Description
cable ofdma-frequency-unused-band	Set the frequency range in the unused band.

cable ofdma-frequency-unused-band

To configure frequencies in unused band, use the **cable ofdma-frequency-unused-band** command in controller configuration mode.

cable ofdma-frequency-unused-band *start value end value*

Syntax Description

<i>start value</i>	Specify the start value of the frequency range.
<i>end value</i>	Specify the end value of the frequency range.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Unused bands apply to OFDMA channels only. OFDMA channel does not use frequencies in unused band set by the **cable ofdma-frequency-unused-band** command for data traffic, but can send probes in them.

Related Commands

Command	Description
cable ofdma-frequency-exclusion-band	Set the frequency range to be excluded from all OFDMA channels on a port.

cable power

To manually power a cable interface line card on or off on a Cisco uBR10012 router, use the **cable power** command in privileged EXEC mode.

cable power [**on**| **off**] *slot/card*

Syntax Description

on	Turns on power to the specified cable interface line card.
off	Turns off power to the specified cable interface line card. Power to that particular card slot remains off until power is turned back on using the cable power on version of this command.
<i>slot/card</i>	Specifies the slot and card number for the desired cable interface card number. The valid range for <i>slot</i> is 5 to 8 and for <i>card</i> is 0 or 1.

Command Default

Cable interface line cards are powered on by default when the card is inserted into the chassis slot.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)BC1b	This command was introduced for the Cisco uBR10012 router.
12.2(8)BC1	This command is disabled if a working TCC+ card is not present in the Cisco uBR10012 router.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This command is typically not used during normal operations, but it can be used for lab, diagnostic, and troubleshooting purposes. For example, using this command to first power off and then power on a card is functionally equivalent to performing an online insertion and removal (OIR) of the card.

Be aware of the following points when using this command:

- Using the **cable power off** command is functionally equivalent to disconnect the cables from the card's upstream and downstream connectors and then removing the card from the chassis. When you use this command to turn off power to a card, the output for the **show interface cable** command for that card will display the message "Hardware is not present."



Note

You can also use the LC Power off Status Reg and Line Card Presence Status Reg fields in the **show controllers clock-reference** command to determine whether a cable interface line card is actually present in the chassis and whether it has been powered on or off.

- Powering off a cable interface line card automatically drops all sessions with the cable modems that are using that card's upstreams and downstreams. Do not use this command on a live network unless this is what you intend.
- All cards are powered on when you upgrade to a new software image for the Cisco uBR10012 router, even if a card had previously been powered off using the **cable power off** command.
- You can turn power both on and off to a cable interface line card slot, even if a card is not physically present in the slot.
- This is the only CLI command that actually powers off a card. The **hw module reset** command appears to perform a similar function, but it performs only the equivalent of issuing the **shutdown** and **no shutdown** commands on the card.
- When power is turned off for a cable interface line card, the power to that card slot will remain off until the **cable power on** command is used to turn the power back on. If you insert a cable interface card in to a slot that had been previously powered down, you will have to use the **cable power on** command to turn on power before being able to use the card.
- This command requires that a working TCC+ card be present because the TCC+ card controls and monitors the operation of the cable interface line cards. In Cisco IOS Release 12.2(8)BC1 and later, this command is disabled if a working TCC+ card is not present in the router.



Note

The Cisco uBR10012 router requires a working TCC+ card for normal operations. Using the router without a working TCC+ card is not a supported configuration.

Examples

The following example shows how to power off the first cable interface card in a Cisco uBR10012 chassis (card 5, slot 0). It also shows the output from the **show interface cable** command, with a line that indicates that the hardware is not present.

```
router# cable power off 5/0

Line Card 5/0 is POWERED OFF
router# show int c5/0/0

Cable5/0/0 is down, line protocol is down
Hardware is not present
Hardware is UBR10012 CLC, address is 0005.00e0.2f14 (bia 0005.00e0.2f14)
Internet address is 10.20.42.1/24
MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec,
```



```

reliability 255/255, txload 1/255, rxload 1/255
...
router#

```



Note The **show interface cable** command will not display output for a card that is not physically present, so if you can use the **show interface cable** command but it indicates that the hardware is not present, this usually means that power to the card has been turned off using the **cable power off** command.

The following example shows the error message that results when you attempt to power on or off a cable interface card that is not physically present in the chassis:

```

router# cable power off 6/1
Line Card 6/1 is not present
router#

```



Note Power is still turned on or off to a cable interface line card slot, even when the card is not physically present in that slot.

Related Commands

Command	Description
hw module reset	Resets a line card, performing the equivalent of the shutdown , no shutdown commands.
show controllers clock-reference	Displays status information from the TCC+ card, including whether a line card is physically present and whether power has been turned off to its slot.
show interface cable	Displays configuration and status information for a cable interface line card.
show version	Displays the basic configuration of the router, including whether an active TCC+ card is present.
shutdown	Disables or enables the interface on a line card.

cable pre-equalization exclude

To exclude a cable modem (CM) from pre-equalization during registration with the Cisco CMTS router, use the **cable pre-equalization exclude** command in global configuration mode. To remove exclusion for the specified cable modem or interface, use the **no** form of this command.

cable pre-equalization exclude {modem *mac-addr*| *oui id*}

no cable pre-equalization exclude {modem *mac-addr*| *oui id*}

Syntax Description

modem <i>mac-addr</i>	Excludes the cable modem with the specified MAC address from pre-equalization during cable modem registration.
oui <i>id</i>	Excludes the specified Organizational Unique Identifier (OUI) from pre-equalization during cable modem registration.

Command Default

Pre-equalization is disabled by default on a Cisco CMTS router, and for cable modems that have a valid and operational DOCSIS configuration file.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(17a)BC	This command was introduced to the Cisco uBR10012 router and the Cisco uBR7246VXR router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Use the **cable pre-equalization exclude** command to disable pre-equalization for DOCSIS 1.1 CMs that claim pre-equalization support but do not properly implement pre-equalization functions.

To enable pre-equalization, use the **cable upstream equalization-coefficient** interface configuration command. Pre-equalization starts when a cable modem that supports DOCSIS 1.1 or above sends the CMTS router a ranging request message indicating that pre-equalization is possible.

The following example of output from the **show cable modem verbose** command shows which modems are indicating pre-equalizer support during the DOCSIS registration process. In this example, the first two modems

are capable of pre-equalization support, and the last two modems support DOCSIS 1.0, which does not support pre-equalization. You do not need to use the **cable pre-equalization exclude** command for DOCSIS 1.0 CMs.

```
Router# show cable modem verbose | include MAC Address|Equalizer
MAC Address          : 0019.474a.c4b0
Transmit Equalizer Support : {Taps/Symbol= 1, Num of Taps= 24}
MAC Address          : 0019.474a.c498
Transmit Equalizer Support : {Taps/Symbol= 1, Num of Taps= 24}
MAC Address          : 0020.40dc.4ce4
Transmit Equalizer Support : {Taps/Symbol= 0, Num of Taps= 0}
MAC Address          : 0020.4077.21a0
Transmit Equalizer Support : {Taps/Symbol= 0, Num of Taps= 0}
```

Exclusion is supported for a specified DOCSIS 1.1 cable modem, or for a specified OUI value for the entire interface. Removing the **cable pre-equalization exclude** configuration returns the cable modem or interface to normal pre-equalization processes during cable modem registration.

Examples

The following example configures pre-equalization to be excluded for the specified cable modem. Pre-equalization data is not sent for the corresponding cable modem:

```
Router(config)# cable pre-equalization exclude modem 1111.2222.3333
```

The following example configures pre-equalization to be excluded for the specified OUI value of the entire interface. Pre-equalization data is not sent for the corresponding OUI value of the entire interface:

```
Router(config)# cable pre-equalization exclude oui
00.09.04
```

The following series of commands configures pre-equalization on the Cisco uBR10012 router with MC5X20U BPEs. On the PRE Console, configure the following commands.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.04
Router(config)# end
Router# show run
Router# show running-config | include oui
cable pre-equalization exclude oui 00.09.04
Router#
```

On the line card console for the same Cisco uBR10012 router, verify the configuration with the following command:

```
Linecard# show running-config | include oui
cable pre-equalization exclude oui 00.09.04
```

The following series of commands configures pre-equalization on the Cisco uBR7246VXR router with MC28U cable interface line cards. On the Network Processing Engine (NPE) console, configure and verify with the following commands.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.24
Router(config)# end
Router#show run
02:58:10: %SYS-5-CONFIG_I: Configured from console by consolen
Router# show running-config | include oui
cable pre-equalization exclude oui 00.09.24
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
Linecard# show running-config | include oui
cable pre-equalization exclude oui 00.09.24
```

After either of these exclusion methods for pre-equalization are configured, you can verify that all ranging messages do not include pre-equalization data. Use the following **debug** commands in global configuration mode:

- **debug cable range**
- **debug cable interface** *cx/x/x mac-addr*

Verify the ranging message for the non-excluded cable modems include pre-equalization data, and for the excluded cable modems, the ranging messages do not include such data.

The following example removes pre-equalization exclusion for the specified OUI and interface. This results in the cable modem or OUI to return to normal pre-equalization functions. Ranging messages resume sending pre-equalization data.

```
Router(config)# no cable pre-equalization exclude {modem mac-addr | oui id}
```

You can verify removal of this feature using the **debug cable interface** command.

Related Commands

Command	Description
debug cable interface	Verifies pre-equalization data and configurations.
debug cable range	Verifies ranging messages for pre-equalization.

cable primary-sflow-qos11 keep

To preserve the traffic counters for primary service flows after a CM that was provisioned for DOCSIS 1.1 quality of service (QoS) goes offline, use the **cable primary-sflow-qos11 keep** command in global configuration mode. To return to the default configuration and reset the counters to zero when a DOCSIS 1.1-provisioned CM goes offline, use the **no** form of this command.

cable primary-sflow-qos11 keep {all| snmp-only}

no cable primary-sflow-qos11 keep

Syntax Description

all	Preserves all primary service flow traffic counters when a DOCSIS 1.1-provisioned CM goes offline. This includes the counters displayed by CLI commands and counters that are obtained through SNMP requests.
snmp-only	Preserves only the primary service flow traffic counters that are obtained through SNMP requests. The counters displayed by CLI commands are reset to zero when a DOCSIS 1.1-provisioned CM goes offline.

Command Default

Primary service flow traffic counters are not preserved after a DOCSIS 1.1-provisioned CM goes offline (**no cable primary-sflow-qos11 keep**). Service-flow information is always preserved for DOCSIS 1.0-provisioned CMs, regardless of the configuration of this command.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)CX, 12.2(15)BC2	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

By default, when a CM that is provisioned for DOCSIS 1.1 quality of service (QoS) service flows goes offline, the CMTS deletes all service flow information, including traffic counters, that correspond to that CM. The **cable primary-sflow-qos11 keep** command preserves the service flow traffic counters after a DOCSIS 1.1-provisioned CM goes offline and then comes back online. This allows service providers to track the total usage of CMs over a period of time, regardless of the number of times the CMs go offline and reboot.

**Note**

This command affects only CMs that are provisioned for DOCSIS 1.1 operations and that are currently online all cable interfaces on the Cisco CMTS. Information is not preserved for DOCSIS 1.1-provisioned CMs that went offline before this command was given. The service-flow information for CMs that are provisioned for DOCSIS 1.0 operations is always preserved, regardless of how this command is configured.

Examples

The following example shows how to preserve both the CLI and SNMP service flow counters when a DOCSIS 1.1-provisioned CM goes offline:

```
Router(config)# cable primary-sflow-qos11 keep all
Router(config)#
```

The following example shows how to preserve only the SNMP-based service flow counters when a DOCSIS 1.1-provisioned CM goes offline. The CLI-based counters are still reset to zero when this CM goes offline.

```
Router(config)# cable primary-sflow-qos11 keep snmp-only
Router(config)#
```

The following example shows how to disable this command and return to the default behavior, which is to reset all CLI-based and SNMP-based counters when a DOCSIS 1.1-provisioned CM goes offline.

```
Router(config)# no cable primary-sflow-qos11 keep
Router(config)#
```

Related Commands

Command	Description
cable sflog	Enables service flow logging and configures the number and duration of entries in the log.
show cable modem counters	Displays downstream and upstream traffic counters for one or more CMs.

cable privacy

To enable and configure BPI or BPI+ encryption, use the **cable privacy** command in cable interface configuration mode. To disable privacy or to remove a particular configuration, use the **no** form of this command.

Cisco uBR Series Router

cable privacy [**accept-self-signed-certificate**| **authenticate-modem**| **authorize-multicast**| **mandatory**| **oaep-support**| **dsx-support**| **retain-failed-certificates**| **skip-validity-period**]

no cable privacy [**accept-self-signed-certificate**| **authenticate-modem**| **authorize-multicast**| **mandatory**| **oaep-support**| **dsx-support**| **retain-failed-certificates**| **skip-validity-period**]

Cisco cBR Series Router

cable privacy [**accept-self-signed-certificate**| **mandatory**| **oaep-support**| **dsx-support**| **retain-failed-certificates**| **skip-validity-period**]

no cable privacy [**accept-self-signed-certificate**| **mandatory**| **oaep-support**| **dsx-support**| **retain-failed-certificates**| **skip-validity-period**]

Syntax Description

accept-self-signed-certificate	(Optional) Allows cable modems to register using self-signed manufacturer certificates, as opposed to a manufacturer certificate that is chained to the DOCSIS root certificate.
authenticate-modem (for uBR series router)	(Optional) Uses AAA protocols in conjunction with BPI to authenticate all CMs.
authorize-multicast (for uBR series router)	(Optional) Uses AAA protocols with baseline privacy interface (BPI) to authorize all multicast stream (IGMP) join requests.
mandatory	(Optional) Requires baseline privacy be active for all CMs with BPI/BPI+ enabled in their DOCSIS configuration files or the CMs are forced to go offline. If a CM does not have BPI enabled in its DOCSIS configuration file, it will be allowed online without BPI.
oaep-support	(Optional) Enables Optimal Asymmetric Encryption Padding (OAEP) BPI+ encryption.
dsx-support	(Optional) Enables encryption for dynamic services SIDs.
retain-failed-certificates	(Optional) Allows to retain failed certificates.

skip-validity-period	(Optional) Enables to skip certificate validity period.
-----------------------------	---

Command Default

The encryption priority defaults to 128bit AES, 56bit DES, 40bit DES depending on modem capability. The CMTS treats self-signed manufacturer certificates as untrusted. Untrusted certificates are not retained by the CMTS.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1 T	This command was introduced.
12.1(4)CX, 12.2(1)XF1, 12.2(4)BC1	Added the dsx-support and oaep-support keywords as part of support for BPI+ encryption.
12.2(11)BC1	Changed the accept-self-signed-certificate option from a global configuration option to a cable interface option.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCC	This command was modified. Added the retain-failed-certificates and skip-validity-period keywords. Removed the 40-bit-des keyword.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers. The authenticate-modem and authorize-multicast keywords were removed.

Usage Guidelines

This command is applicable only on images that support BPI or BPI+ encryption.

**Note**

The **cable privacy accept-self-signed-certificate** command affects only those CMs that register after you give the command. For example, if you give the **no cable privacy accept-self-signed-certificate** command so that CMs cannot register using self-signed certificates, you must then issue the **clear cable modem all reset** command to force all CMs reregister using certificates that are chained to the DOCSIS root certificate.

Providing Self-Signed Certificates

Cisco IOS Release 12.2(33)SCC and later releases allow self-signed CA certificates to be programmed on the file system to allow specific modems to authenticate. This is frequently used for test equipment and modems that are not DOCSIS compliant.

To provide self-signed CA certificates, perform the following steps:

- 1 Acquire the CA certificate in Distinguished Encoding Rules (DER) format. This can be supplied by the manufacturer or retrieved from the cable modem.

- 2 Store the self-signed CA certificate in the bootflash by naming it “trusted-cert-scrt n”, for example “trusted-cert-scrt1” or “trusted-cert-scrt2”.
- 3 Ensure that **cable privacy accept-self-signed-certificate** command is not enabled.
- 4 Save the configuration.
- 5 Reboot the router.

The router reads the new files and the self-signed cable modem comes online.

Examples

The following example shows how to force baseline privacy interface (BPI) to be used for all CMs on a particular cable interface:

```
Router(config)# interface cable 6/0/0
Router(config-if)# cable privacy mandatory
```

The following example shows how to turn on the BPI modem authentication for an interface:

```
Router(config)# interface cable 6/0/1
Router(config-if)# cable privacy authenticate-modem
```

The following example shows how to turn on BPI multicast authorization on a particular cable interface on Cisco uBR series router:

```
Router(config)# interface cable 1/0
Router(config-if)# cable privacy authorize-multicast
```

The following example shows how to allow CMs to register with self-signed certificates on a particular cable interface:

```
Router(config)# interface cable 7/0/0
Router(config-if)# cable privacy accept-self-signed-certificate
```

The following example shows how to allow CMs to enable privacy DSX support on a particular cable interface:

```
Router(config)# interface cable 6/0/0
Router(config-if)# cable privacy dsx-support
```

The following example shows how to allow CMs to enable OAEP support on a particular cable interface:

```
Router(config)# interface cable 6/0/0
Router(config-if)# cable privacy oaep-support
```

The following example shows how to allow CMs to retain failed certificates on a particular cable interface:

```
Router(config)# interface cable 6/0/0
Router(config-if)# cable privacy
retain-failed-certificates
```

The following example shows how to allow CMs to skip certificate validity period on a particular cable interface:

```
Router(config)# interface cable 6/0/0
Router(config-if)# cable privacy
skip-vailidity-period
```

Related Commands

Command	Description
cable privacy add-certificate	Adds CM certificates for BPI+ encryption.
cable privacy eae-policy	Selects Early Authentication and Encryption policy.

Command	Description
cable privacy hotlist	Adds a CM certificate to the DOCSIS hotlist so that it is no longer accepted.
cable privacy kek	Sets key encryption keys and timeout periods.
cable privacy tek	Sets traffic encryption keys and timeout periods.
show cable privacy	Displays information about BPI status and operation.
debug cable privacy	Displays debug messages for BPI operation.

cable privacy bpi-plus-enforce



Note Effective with Cisco IOS Release 12.2(33)SCD5, the **cable privacy bpi-plus-enforce** command is replaced with the **cable privacy bpi-plus-policy** command. For more information, see the **cable privacy bpi-plus-policy** command.

To mandate that a cable modem provisioned in DOCSIS 1.1 or higher must register with DOCSIS Baseline Privacy Interface Plus (BPI+), and not use the earlier DOCSIS BPI, use the **cable privacy bpi-plus-enforce** command in global configuration mode. To remove this configuration, use the **no** form of this command.

cable privacy bpi-plus-enforce

no cable privacy bpi-plus-enforce

Syntax Description

This command has no arguments or keywords.

Command Default

The **cable privacy bpi-plus-enforce** command is not enabled by default, but must be configured for optimal DOCSIS BPI+ security.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(21)BC	This command was introduced.
12.2(33)SCD5	This command was replaced with the cable privacy bpi-plus-policy command .
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable privacy bpi-plus-enforce** command enables the Cisco CMTS router to detect cloned cable modems and eliminate denial-of-service (DOS) attacks that are caused by cloned cable modems.

If the cable modem is not provisioned to use DOCSIS BPI or BPI+ security certificates, then the existing behavior of the Cisco CMTS router remains unchanged. The Cisco CMTS router does not attempt to distinguish between two cable modems if neither is provisioned for BPI+ security.



Note The non-DOCSIS compliant cable modems that are commonly available contain an option to force registration in DOCSIS BPI, as opposed to DOCSIS BPI+ mode, even in DOCSIS 1.1-provisioned networks.

Examples

The following example illustrates logging messages that are created with the detection of cloned cable modems:

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been moved
from interface Cable7/0/1 to interface Cable7/0/0.
Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
access detected at Cable7/0/0 interface
```

Related Commands

Command	Description
cable logging layer2events	Saves selected (low priority) DOCSIS events that are specified in the Cisco CMTS MIB registry to the cable logging buffer (instead of to the general logging buffer).
cable privacy bpi-plus-policy	Configures the BPI+ enforcement policies on a Cisco CMTS router.
show cable logging	Displays the log of messages about bad IP source addresses or DOCSIS layer events on the cable interfaces.
show cable modem	Displays information for registered and non-registered cable modems on the Cisco CMTS.

cable privacy bpi-plus-exclude

To exclude cable modems from the Baseline Privacy Interface Plus (BPI+) enforcement policies configured on a Cisco CMTS router, use the **cable privacy bpi-plus-exclude** command in global configuration mode. To disable this configuration, use the **no** form of this command.

cable privacy bpi-plus-exclude *mac-address* [*address-mask*]

no cable privacy bpi-plus-exclude *mac-address* [*address-mask*]

Syntax Description

<i>mac-address</i>	Cable modem MAC address.
<i>address-mask</i>	(Optional) Cable modem subnet.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCD5	This command was introduced.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

You can exclude individual cable modems, which are compliant with DOCSIS 1.0 and later versions, from the BPI+ enforcement policy based on their MAC addresses on a per-MAC domain basis. If a cable modem is added to the exclusion list, the Cisco CMTS router does not enforce the BPI+ enforcement policy on that cable modem. You can exclude a maximum of 30 cable modems per MAC domain.

Examples

The following example shows how to exclude a cable modem from the BPI+ enforcement policy based on its MAC address:

```
Router# configure terminal
Router(config)# cable privacy bpi-plus-exclude 0010.9571.03ab
```

Related Commands

Command	Description
cable privacy bpi-plus-policy	Configures the BPI+ enforcement policy on a Cisco CMTS router.

Command	Description
show interface cable privacy	Displays baseline privacy information.

cable privacy bpi-plus-policy

To configure the Baseline Privacy Interface Plus (BPI+) enforcement policies on a Cisco CMTS router, use the **cable privacy bpi-plus-policy** command in cable interface configuration mode. To disable this configuration, use the **no** form of this command.

```
cable privacy bpi-plus-policy {capable-enforcement| d11-enabled-enforcement| d11-enforcement|
total-enforcement}
```

```
no privacy bpi-plus-policy {capable-enforcement| d11-enabled-enforcement| d11-enforcement|
total-enforcement}
```

Syntax Description

capable-enforcement	Specifies that BPI+ enforcement is required on all BPI+ capable cable modems that are BPI+ enabled and provisioned with DOCSIS1.1 configuration file (Policy 1).
d11-enabled-enforcement	Specifies that BPI+ enforcement is required on all cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29 (Policy 2).
d11-enforcement	Specifies that BPI+ enforcement is required on all cable modems that are compliant with DOCSIS 1.1 and later versions (Policy 3).
total-enforcement	Specifies that BPI+ enforcement is required on all cable modems (Policy 4).

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCD5	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable privacy bpi-plus-policy** command replaced the **cable privacy bpi-plus-enforce** command in Cisco IOS Release 12.2(33)SCD5. If you upgrade from an earlier Cisco IOS Release to Cisco IOS Release

12.2(33)SCD5 and later, the existing BPI+ enforcement configuration is disabled by default during the upgrade. You must reconfigure the BPI+ enforcement policy using the **cable privacy bpi-plus-policy** command.

You can configure only one enforcement policy at a time per MAC domain. If you configure one policy after another, the latest policy supersedes the already existing policy. For example, if you want Policy 2 to take over Policy 1, you can directly configure the former without disabling the latter.

Examples

The following example shows how to configure BPI+ enforcement policies on the cable interface 3/0 on the Cisco uBR7246VXR router:

```
Router# configure terminal
Router(config)# interface cable 3/0
Router(config-if)# cable privacy bpi-plus-policy capable-enforcement
Router(config-if)# cable privacy bpi-plus-policy dll-enabled-enforcement
Router(config-if)# cable privacy bpi-plus-policy dll-enforcement
Router(config-if)# cable privacy bpi-plus-policy total-enforcement
```

Related Commands

Command	Description
cable privacy bpi-plus-exclude	Excludes individual cable modems from BPI+ enforcement policies based on their MAC addresses.
show interface cable privacy	Displays baseline privacy information.

cable privacy clone-detect

To enable the clone modem functionality for a cable modem, use the **cable privacy clone-detect** command in global configuration mode. To disable clone modem functionality, use the **no** form of this command.

cable privacy clone-detect

no cable privacy clone-detect

Syntax Description This command has no keywords or arguments.

Command Default The clone modem functionality is enabled .

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Examples The following example shows how to enable the clone modem functionality, so that the cloned cable modems cannot register with the CMTS:

```
Router# configure terminal
Router(config)# cable privacy clone-detect
```

Related Commands	Command	Description
	cable privacy	Enables and configures BPI+ encryption on a cable interface.
	(Not supported for Cisco uBR10K Series and cBR Series Converged Broadband Routers) cable privacy bpi-plus-enforce	Specifies that a cable modem provisioned in DOCSIS 1.1 or higher must register with DOCSIS BPI+, and not use the earlier DOCSIS BPI.
	cable logging layer2events	Saves selected (low priority) DOCSIS events that are specified in the Cisco CMTS MIB registry to the cable logging buffer (not of the general logging buffer).

Command	Description
show cable logging	Displays the log of messages, about bad IP source addresses or DOCSIS-layer events, on the cable interfaces.
show cable modem	Displays information for registered and non-registered cable modems on the Cisco CMTS.
show running-config interface cable	Displays the bundles that are configured on a Cisco CMTS router showing the running configuration for each of the cable interfaces.

cable privacy eae-exclude

To force a cable modem to register without an Early Authentication and Encryption (EAE) and add it to the EAE exclusion list, use the **cable privacy eae-exclude** command in global configuration mode. To remove a particular CM from the exclusion list, use the **no** form of this command.

cable privacy eae-exclude *cm-mac-address* [*mask*]

no cable privacy eae-exclude *cm-mac-address* [*mask*]

Syntax Description

<i>cm-mac-address</i>	Hardware (MAC) address of a specific cable modem to be added to the EAE exclusion list.
<i>mask</i>	(Optional) Mask value for the cable modem.

Command Default

The EAE exclusion list does not contain any MAC address.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCC	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The exclusion list is mainly used to debug issues with specific cable modems.

Examples

The following example shows how to add a CM with the MAC address of 00C0.8345.de51 to the EAE exclusion list, so that this particular CM cannot register with the CMTS:

```
Router# configure terminal
Router(config)# cable privacy eae-exclude 00C0.8345.de51
Router(config)#
```

Related Commands

Command	Description
cable privacy	Enables and configures BPI+ encryption on a cable interface.

Command	Description
cable privacy kek	Sets key encryption keys and timeout periods.
cable privacy tek	Sets traffic encryption keys and timeout periods.
show cable privacy	Displays information about BPI status and operation.

cable privacy eae-policy

To enable the Early Authentication and Encryption (EAE) policy, use the **cable privacy eae-policy** command in cable interface configuration mode. To disable the EAE policy, use the **no** form of this command.

cable privacy eae-policy {**capability-enforcement**| **disable-enforcement**| **ranging-enforcement**| **total-enforcement**}

no cable privacy eae-policy {**capability-enforcement**| **disable-enforcement**| **ranging-enforcement**| **total-enforcement**}

Syntax Description

capability-enforcement	Enforces EAE on capable modems.
disable-enforcement	Disables EAE thereby preventing the CMTS from enforcing EAE on any cable modem.
ranging-enforcement	Enforces EAE only on DOCSIS 3.0 modems.
total-enforcement	Enforces EAE on all cable modems.

Command Default

EAE policy is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCC	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The EAE policy is applied on a MAC domain and the policies are mutually exclusive. The CMTS enforces EAE only on CMs that initialize on a downstream channel on which the CMTS is transmitting MAC Domain Descriptor (MDD) messages.

The EAE exclusion list is a global list and is created on all line cards as part of the DOCSIS 3.0 specifications. Cable modems in the EAE exclusion list are always exempted from EAE enforcement. If the CMTS receives an authorization request before the CM is registered in the EAE exclusion list, the CMTS rejects that request.

**Note**

When Early Authentication and Encryption is enabled in Cisco cBR-8 router, BPI will revert back to DES-56 even if the hardware supports AES-128.

Examples

The following example shows how to enforce EAE policy on capable modems:

```
Router(config)# interface cable 3/0/0
Router(config-if)# cable privacy eae-policy capability-enforcement
```

The following example shows how to disable EAE policy so that the CMTS does not enforce EAE policy on any cable modem:

```
Router(config)# interface cable 3/0/0
Router(config-if)# cable privacy eae-policy disable-enforcement
```

The following example shows how to enforce EAE policy on DOCSIS 3.0 modems only:

```
Router(config)# interface cable 3/0/0
Router(config-if)# cable privacy eae-policy ranging-enforcement
```

The following example shows how to enforce EAE policy on all cable modems:

```
Router(config)# interface cable 3/0/0
Router(config-if)# cable privacy eae-policy total-enforcement
```

Related Commands

Command	Description
cable privacy exe-exclude	Adds the CM to be excluded from EAE policy enforcement.
cable privacy hotlist	Adds a CM certificate to the DOCSIS hotlist so that it is no longer accepted.
cable privacy kek	Sets key encryption keys and timeout periods.
cable privacy tek	Sets traffic encryption keys and timeout periods.
show cable privacy	Displays information about BPI status and operation.

cable privacy encrypt-alg-priority

To specify the order in which to use the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm, use the **cable privacy encrypt-alg-priority** command in global configuration mode. To remove the encryption algorithm and revert to the default priority, use the **no** form of this command.

```
cable privacy encrypt-alg-priority {aes128-des40-des56| aes128-des56-des40| des40-aes128-des56|
des40-des56-aes128| des56-aes128-des40| des56-des40-aes128}
```

```
no cable privacy encrypt-alg-priority
```

Syntax Description

aes128-des40-des56	Specifies the order of the encryption algorithm priority. AES with a 128-bit block is given the highest priority, followed by DES with 40-bit block size, and DES with 56-bit block size.
aes128-des56-des40	Specifies the order of the encryption algorithm priority. AES with a 128-bit block size is given the highest priority, followed by DES with 56-bit block size, DES with 40-bit block size.
des40-aes128-des56	Specifies the order of the encryption algorithm priority. DES with 40-bit block size is given the highest priority, followed by AES with a 128-bit block size, and DES with 56-bit block size.
des40-des56-aes128	Specifies the order of the encryption algorithm priority. DES with 40-bit block size is given the highest priority, followed by DES with 56-bit block size and AES with 128-bit block size.
des56-aes128-des40	Specifies the order of the encryption algorithm priority. DES with 56-bit block size is given the highest priority, followed by AES with a 128-bit block size, and DES with 40-bit block size.
des56-des40-aes128	Specifies the order of the encryption algorithm priority. DES with 56-bit block size is given the highest priority, followed by DES with 40-bit block size, and AES with a 128-bit block size.

Command Default Default value is aes128-des56-des40.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines Use this command to specify the order of the encryption algorithm priority. When Early Authentication and Encryption is enabled in Cisco cBR-8 router, BPI will revert back to DES-56 even if the hardware supports AES-128.

Examples The following example shows how to assign AES the highest priority, followed by 40-bit DES, and 56-bit DES.

```
Router# configure terminal
Router(config)# cable privacy encrypt-alg-priority aes128-des40-des56
Router(config)#
```

Related Commands

Command	Description
cable privacy	Enables and configures BPI+ encryption on a cable interface.
cable privacy kek	Sets key encryption keys and timeout periods.
cable privacy tek	Sets traffic encryption keys and timeout periods.
show cable privacy	Displays information about BPI status and operation.

cable privacy hotlist

To mark a manufacturer's or CM certificate as untrusted and add them to the CMTS hotlist of invalid certificates, thereby preventing those CMs or host's from registering, use the **cable privacy hotlist** command in global configuration mode. To remove a particular CM or manufacturer's certificate from the hotlist, use the **no** form of this command.

cable privacy hotlist {**cm** *mac-address*| **manufacturer** *cert-serial-number*}

no cable privacy hotlist {**cm** *mac-address*| **manufacturer** *cert-serial-number*}

Cisco cBR Series Converged Broadband Routers

cable privacy hotlist {**cm** *mac-address*| **host** *mac-address* }

no cable privacy hotlist {**cm** *mac-address*| **host** *mac-address* }

Syntax Description

cm <i>mac-address</i>	Specifies the MAC address for the CM to be added to the hotlist. The <i>mac-address</i> should be specified as a hexadecimal string, without periods or other separators. In Cisco IOS Release 12.2(15)BC2 and later releases, you can also specify it as three sets of hexadecimal digits, separated by periods.
manufacturer <i>cert-serial-number</i>	Specifies the serial number for the particular manufacturer CA certificate. The <i>cert-serial-number</i> should be specified as a hexadecimal string up to 32 bytes in length. Enter multiple lines as needed, and use a blank line to terminate the string.
host <i>mac-address</i>	Specifies the MAC address for the host to be added to the hotlist. The <i>mac-address</i> should be specified as a hexadecimal string, without periods or other separators. In Cisco IOS Release 12.2(15)BC2 and later releases, you can also specify it as three sets of hexadecimal digits, separated by periods.

Command Default

The CMTS hotlist does not contain any certificates.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)CX, 12.2(1)XF1, 12.2(4)BC1	This command was introduced for the Cisco uBR7100 series and Cisco uBR7200 series routers.

Release	Modification
12.2(11)BC1	The accept-self-signed-certificate option was moved to the cable privacy cable interface command.
12.2(15)BC2	The mac-address can be specified in the canonical form of three pairs of hexadecimal digits, separated by periods (for example, 0000.0001.0002).
12.2(33)SCB5	This command was integrated into the 12.2SC release train.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers. The host keyword was added.

Usage Guidelines

The **cable privacy hotlist** command is used to configure the following features:

- [DOCSIS 1.1 for the Cisco CMTS Routers](#)

This command is applicable only on images that support BPI or BPI+ encryption.



Note

The **cable privacy hotlist** command is not supported on the Cisco uBR10012 router running Cisco IOS releases prior to Cisco IOS release 12.3(23)BC9, Cisco IOS release 12.2(33)SCB5, and Cisco IOS release 12.2(33)SCC. To add a manufacturer's or CM certificate to the hotlist on the Cisco uBR10012 router, use SNMP commands to set the appropriate attributes in DOCS-BPI-PLUS-MIB.

Examples

The following command adds the CM certificate with the MAC address of 00C0.8345.de51 to the hotlist, so that this particular CM cannot register with the CMTS:

```
Router# configure terminal
Router(config)# cable privacy hotlist cm 00C08345de51
Router(config)#
```

The following example adds a manufacturer CA certificate into the BPI+ hotlist, so that the CMTS will reject any CM attempting to register with a certificate from that particular manufacturer:

```
Router# configure terminal
Router(config)# cable privacy hotlist manufacturer 3435414631413439383335453731423733333643
```

Related Commands

Command	Description
cable privacy	Enables and configures BPI+ encryption on a cable interface.
cable privacy add-certificate	Adds CM certificates for BPI+ encryption.
option	Determines whether a specific CM is online.
cable privacy kek	Sets key encryption keys and timeout periods.

Command	Description
cable privacy tek	Sets traffic encryption keys and timeout periods.
show cable privacy	Displays information about BPI status and operation.
debug cable privacy	Displays debug messages for BPI operation.

cable privacy kek

To set key encryption keys (KEKs) life-time values for baseline privacy on an HFC network, use the **cable privacy kek** command in cable interface configuration mode. To restore the default values, use the **no** form of this command.



Note

This command is applicable only on images that support BPI or BPI+ encryption.

cable privacy kek life-time [*seconds*]

no cable privacy kek life-time

Syntax Description

life-time <i>seconds</i>	(Optional) Length of the key encryption life-time in seconds. The valid range is 300 to 604,800. The default is 604,800 seconds (7 days).
---------------------------------	---

Command Default

The **life-time** option to 604,800 seconds (7 days).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3 XA	This command was introduced.
12.1(4)CX, 12.2(1)XF1, 12.2(4)BC1	The valid range for both options was changed to support DOCSIS 1.1 and BPI+ encryption.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Baseline privacy on an HFC network is configured with key encryption keys (KEKs) and traffic encryption keys (TEKs). The encryption is based on 40-bit or 56-bit data encryption standard (DES) encryption algorithms.

A KEK is assigned to a cable modem based on the cable modem service identifier (SID) and permits the cable modem to connect to the Cisco CMTS when baseline privacy is activated. KEKs can be set to expire based a life-time value.

The **life-time** keyword is used to assign a more permanent key to a cable modem.

A cable modem that has a life-time key assigned by the Cisco CMTS requests a new key before the current one expires.

Examples

The following example shows how to set the KEK privacy life-time to 750,000 seconds:

**Note**

CableLabs recommended operational KEK life time is:

- Minimum 1 day
- Normal 7 days
- Maximum 70 days and
- 300 seconds for integration testing alone

```
Router(config)# interface cable c3/0/0
Router(config-if)# cable privacy kek life-time 750000
Router(config-if)#
```

Related Commands

Command	Description
cable privacy add-certificate	Configures certificates for BPI+ encryption.
cable privacy	Enables and configures BPI+ encryption on a cable interface.
cable privacy tek	Sets traffic encryption keys and timeout periods.
option	Determines whether a specific CM is online.
privacy	Configures the BPI or BPI+ configuration parameters in a DOCSIS configuration file.
show cable privacy	Displays information about BPI status and operation.
show interface cable privacy	Displays the current values of the KEK and TEK timers for an interface.
debug cable privacy	Displays debug messages for BPI operation.

cable privacy non-mtc-aes128

To allow DOCSIS3.0 cable modem working on non-MTC mode to use AES-128 as BPI encryption algorithms, use the **cable privacy non-mtc-aes128** command in global configuration mode. To disable this feature, use the **no** form of this command.

cable privacy non-mtc-aes128

no cable privacy non-mtc-aes128

Command Default None.

Command Modes Global configuration (config)

Command History	Release	Modification
	IOS-XE 3.18.1SP	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Examples

The following example shows how to add a CM with the MAC address of 00C0.8345.de51 to the EAE exclusion list, so that this particular CM cannot register with the CMTS:

```
Router# configure terminal
Router(config)# cable privacy non-mtc-aes128
Router(config)#
```

cable privacy revocation crl skip-sig-check

To allow the Cisco CMTS router to skip the certification revocation list (CRL) response signature check, use the **cable privacy revocation crl skip-sig-check** command in global configuration mode. To enable CRL signature check, use the **no** form of this command.

cable privacy revocation crl skip-sig-check
no cable privacy revocation crl skip-sig-check

Syntax Description This command has no keywords or arguments.

Command Default The CRL response signature check is enabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines The **cable privacy revocation crl skip-sig-check** command allows you to use the CRL response from the CRL server without validating the signature of the response.

Examples The following example shows how to skip the CRL response signature check:

```
Router(config)# cable privacy revocation crl skip-sig-check
```

Related Commands

Command	Description
cable privacy revocation oosp skip-sig-check	Allows to skip the OOSP response signature check.
cable privacy revocation skip-cm-cert	Allows to disable checking of the CM certificates.
cable privacy revocation timeout	Sets the timeout value of CRL or OOSP response time.
cable privacy revocation enable	Allows to quickly enable privacy revocation checking.
show cable privacy	Displays information about BPI status and operation.

Command	Description
debug cable privacy	Displays debug messages for BPI operation.

cable privacy revocation enable

To quickly enable privacy revocation checking, use the **cable privacy revocation enable** command in global configuration mode. To disable privacy revocation checking, use the **no** form of this command.

cable privacy revocation enable

no cable privacy revocation enable

Syntax Description This command has no keywords or arguments.

Command Default The privacy revocation checking is disabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines This command allows you to quickly enable or disable revocation checking. When you enable revocation checking, it creates the trustpoints for both the EU and US certificates.

Examples The following example shows how to enable revocation checking:

```
Router(config)# cable privacy revocation enable
```

Related Commands	Command	Description
	cable privacy revocation ocsip skip-sig-check	Allows to skip the OCSP response signature check.
	cable privacy revocation skip-cm-cert	Allows to disable checking of the CM certificates.
	cable privacy revocation timeout	Sets the timeout value of CRL or OCSP response time.
	show cable privacy	Displays information about BPI status and operation.
	debug cable privacy	Displays debug messages for BPI operation.

■ cable privacy revocation enable

cable privacy revocation oosp skip-sig-check

To allow the Cisco CMTS router to skip the Online Certificate Status Protocol (OCSP) response signature check, use the **cable privacy revocation oosp skip-sig-check** command in global configuration mode. To enable OCSP signature check, use the **no** form of this command.

cable privacy revocation oosp skip-sig-check

no cable privacy revocation oosp skip-sig-check

Syntax Description This command has no keywords or arguments.

Command Default OCSP response signature check is enabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines The **cable privacy revocation oosp skip-sig-check** command allows you to use the OCSP response from the OCSP responder without validating the signature of the response.

Examples The following example shows how to skip the OCSP response signature check:

```
Router(config)# cable privacy revocation oosp skip-sig-check
```

Related Commands	Command	Description
	cable privacy revocation enable	Allows to quickly enable privacy revocation checking.
	cable privacy revocation skip-cm-cert	Allows to disable checking of the CM certificates.
	cable privacy revocation timeout	Sets the timeout value of CRL or OCSP response time.
	show cable privacy	Displays information about BPI status and operation.
	debug cable privacy	Displays debug messages for BPI operation.

■ cable privacy revocation ocsp skip-sig-check

cable privacy revocation skip-cm-cert

To disable checking of the CM certificates, use the **cable privacy revocation skip-cm-cert** command in global configuration mode. To enable checking of CM certificates, use the **no** form of this command.

cable privacy revocation skip-cm-cert

no cable privacy revocation skip-cm-cert

Syntax Description This command has no keywords or arguments.

Command Default CM certificate checking is enabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Note

Checking CM certificates requires a lot of processing power, which impacts the router performance.

Examples The following example shows how to disable checking of CM certificates:

```
Router(config)# cable privacy revocation skip-cm-cert
```

Related Commands

Command	Description
cable privacy revocation enable	Allows to quickly enable privacy revocation checking.
cable privacy revocation ocsp skip-sig-check	Allows to skip the OCSP response signature check.
cable privacy revocation timeout	Sets the timeout value of CRL or OCSP response time.
show cable privacy	Displays information about BPI status and operation.

Command	Description
debug cable privacy	Displays debug messages for BPI operation.

cable privacy revocation timeout

To set the timeout value of certification revocation list (CRL) or Online Certificate Status Protocol (OCSP) response time for authorization “reply” or “reject” messages, use the **cable privacy revocation timeout** command in global configuration mode. To return to the default timeout value, use the **no** form of this command.

cable privacy revocation timeout

no cable privacy revocation timeout

Syntax Description This command has no keywords or arguments.

Command Default The default timeout value is 1 second.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines This command only takes effect if **cable privacy revocation enable** command is configured. The timeout value for authorization “reply” or “reject” messages in the CM configuration file must be greater than the revocation timeout value.

Examples The following example shows how to set the timeout value for CRL or OCSP response:

```
Router(config)# cable privacy revocation timeout 15
```

Related Commands	Command	Description
	cable privacy revocation enable	Allows to quickly enable privacy revocation checking.
	cable privacy revocation ocsip skip-sig-check	Allows to skip the OCSP response signature check.
	cable privacy revocation skip-cm-cert	Allows to disable checking of the CM certificates.
	show cable privacy	Displays information about BPI status and operation.

Command	Description
debug cable privacy	Displays debug messages for BPI operation.

cable privacy tek

To set traffic encryption keys (TEKs) life-time values for baseline privacy on an HFC network, use the **cable privacy tek** command in cable interface configuration mode. To restore the default value, use the **no** form of this command.


Note

This command is applicable only on images that support BPI or BPI+ encryption.

cable privacy tek life-time [*seconds*]

no cable privacy tek life-time

Syntax Description

life-time <i>seconds</i>	(Optional) Length of the traffic encryption life-time in seconds. The range is 180 to 604,800. The default is 43,200.
---------------------------------	---

Command Default

The **life-time** option to 43200 seconds (12 hours).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3 XA	This command was introduced.
12.1(4)CX, 12.2(1)XF1, 12.2(4)BC1	The valid range for both options was changed to support DOCSIS 1.1 and BPI+ encryption.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Baseline privacy on an HFC network is configured with key encryption keys (KEKs) and traffic encryption keys (TEKs). The encryption is based on 40-bit or 56-bit data encryption standard (DES) or 128-bit AES encryption algorithms.

The TEK is assigned to a CM when its KEK has been established. The TEK is used to encrypt data traffic between the CM and the Cisco CMTS. TEKs can be set to expire based a life-time value.

The **life-time** keyword is used to assign a more permanent key to a CM.

**Note**

CableLabs recommended operational TEK life time is:

- Minimum 30 minutes
- Normal 12 hours
- Maximum 7 days and
- 180 seconds for integration testing alone

A CM that has a life-time key assigned by the Cisco CMTS requests a new key before the current one expires.

Examples

The following example shows how to set the traffic encryption key life-time to 800000 seconds:

```
Router(config)# interface cable c3/0/0
Router(config-if)# cable privacy tek life-time 800000
Router(config-if)#
```

Related Commands

Command	Description
cable privacy add-certificate	Configures certificates for BPI+ encryption.
cable privacy	Enables and configures BPI+ encryption on a cable interface.
cable privacy kek	Sets key encryption keys and timeout periods.
option	Determines whether a specific CM is online.
privacy	Configures the BPI or BPI+ configuration parameters in a DOCSIS configuration file.
show cable privacy	Displays information about BPI status and operation.
show interface cable privacy	Displays the current values of the KEK and TEK timers for an interface.
debug cable privacy	Displays debug messages for BPI operation.

cable profile

To create and configure common profile for service group based configuration of layer 2 (L2) interfaces, use the **cable profile** command. To remove a common profile use the **no** form of the command with the appropriate key words and variables.

cable profile *profile-type* *profile-name*

Syntax Description

<i>profile-type</i>	Configures the profile type for configuration. <ul style="list-style-type: none"> • mac-domain — Selects a MAC domain common profile for configuration. • downstream — Selects a downstream interface common profile to configure. • wideband-interface — Selects a wideband interface common profile to configure. • service-group — Creates fiber-node service group profile.
<i>profile-name</i>	Configures the profile name.

Command Default

Not configured.

Command Modes

Privileged Configuration Mode (config)

Command History

Release	Modification
Cisco IOS-XE 3.17.0S	The command was introduced.

Usage Guidelines

Feature—Service Group Profile Based Configuration for DOCSIS interfaces and fiber nodes.

Use this command to configure the three common profiles — MAC domain, primary downstream channel profile and wideband-cable interface profile. When you enter the profile configuration mode, configure the parameters for the profile. These parameters will be applied when this profile is added to a specific service group profile. This command is used to create the service group profile.

MAC Domain Common Profile

When you enter the MAC domain common profile configuration mode, configure the following using the **cable** command:

- **cable ip-init [apm | dual-stack | ipv4 | ipv6]**
- **cable mrc-mode**
- **cable mtc-mode**

- **cable dynamic-secret** [**lock** | **mark** | **reject**]
- **cable shared-secret** [**0** | **7** | **LINE**]
- **cable privacy bpi-plus-policy** [**capable-enforcement** | **d11-enabled-enforcement** | **d11-enforcement** | **total-enforcement**]
- **cable privacy mandatory**

Primary Downstream Channel Common Profile

When you enter the primary downstream channel common profile configuration mode, configure the following using the **cable** command:

- **cable rf-bandwidth-percent** *percent* [**remaining ratio** *percent*]
- **cable attribute-mask** *mask*

Wideband Interface Common Profile

When you enter the wideband interface common profile configuration mode, configure the following using the **cable** command:

- **cable downstream attribute-mask** *mask*

Global Service Group Profile

When you enter the global service group configuration mode, use the following commands:

- Enter the MAC domain mode using **mac-domain** *mac-domain id* **profile** *mac-domain profile name*
- In the MAC domain mode:
 - Configure the downstream service group channels using the **downstream sg-channel** *group list profile ds profile name upstream group list*
 - Configure the upstream service group channels using the **upstream** *Id* **sg-channel** *sg channel Id*
 - Configure the upstream bonding group by entering the upstream bonding group configuration mode using the **us-bonding-group** *Id* command.
 - In the upstream bonding group configuration mode, use the **upstream** *Id* command to add the upstream channels.
 - In the upstream bonding group configuration mode, use the **attribute** *mask* command to add attribute mask for this upstream bonding group .
- Enter the wideband interface configuration group using the **wideband-interface** *Id* **profile** *BG profile name*
 - In the wideband interface configuration mode, use the **downstream sg-channel** *group list rf-bandwidth-percent percent* command to add the upstream channels.

Examples

This example shows how to configure a MAC domain common profile using the **cable profile** command.

```
Router(config)#cable profile mac-domain md1
Router(config-profile-md)#cable dynamic-secret mark
Router(config-profile-md)#cable shared-secret 0
Router(config-profile-md)#cable ip-init ipv4
```

```

Router(config-profile-md) #cable mtc-mode
Router(config-profile-md) #cable mrc-mode
Router(config-profile-md) #cable privacy mandatory
Router(config-profile-md) #cable privacy bpi-plus-policy total-enforcement

Router(config-profile-md) #exit
Router(config) #

```

Examples

This example shows how to configure a primary downstream channel common profile using the **cable profile** command. Set the attribute mask value and the RF bandwidth percentage for the primary downstream channel profile.

```

Router(config) #cable profile downstream dsl
Router(config-profile-ds) # cable attribute-mask mask
Router(config-profile-ds) # cable rf-bandwidth-percent percent

Router(config-profile-ds) #exit
Router(config) #

```

Examples

This example shows how to configure a wideband interface common profile using the **cable profile** command. Set the attribute mask value for the wideband interface profile using the **downstream** keyword.

```

Router(config) #cable profile wideband-interface BG1
Router(config-profile-wb) # cable downstream attribute-mask mask
Router(config-profile-wb) #exit
Router(config) #

```

Examples

This example shows how to configure a global service group profile using the **cable profile** command. Configure the required MAC domain and wideband interface parameters in the global service group profile configuration mode.

```

Router(config) #cable profile service-group SG-16x8-1_1
Router(config-profile-sg) #cable bundle bundle ID
Router(config-profile-sg) #mac-domain mac-domain ID profile mac-domain profile name
Router(config-profile-sg-md) #downstream sg-channel grouplist profile downstream interface
profile ID
upstream grouplist
Router(config-profile-sg-md) #upstream Id sg-channel sg channel Id
Router(config-profile-sg-md) #us-bonding-group bonding group ID
Router(config-profile-sg-md-usbg) #upstream Id
Router(config-profile-sg-md-usbg) #attributes mask
Router(config-profile-sg-md-usbg) #exit
Router(config-profile-sg-md) #exit
Router(config-profile-sg) #

Router(config-profile-sg) #wideband-interface downstream bonding group id profile
downstream bonding group id
Router(config-profile-sg-bg) #downstream sg-channel grouplist rf-bandwidth-percent
bandwidth percent
Router(config-profile-sg-bg) #end
Router#

```

cable profile rpd-event

To configure an event profile and apply it to RPD, use the **cable profile rpd-event** *profile_id* command in the global configuration mode.

cable profile rpd-event *profile_id* *priority* {0x0| 0x1| 0x2| 0x3}

Syntax Description

rpd-event	Configures an event profile
<i>profile-id</i>	Profile ID for the event.
<i>priority</i>	The type of event. <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
{0x0 0x1 0x2 0x3}	Type of notifications. <ul style="list-style-type: none"> • 0x0—No log • 0x1— Save log in RPD local storage • 0x2—Report to Cisco cBR • 0x3—Save log in RPD local storage and report to Cisco cBR

Command Default

Not configured.

Command Modes

Privileged Configuration Mode (config)

Command History

Release	Modification
Cisco RPD IOS 1.1	The cable profile rpd-event <i>profile_id</i> command was introduced.

Usage Guidelines

RPD Event Profile

The **cable profile rpd-event** *profile_id* command is used to configure an RPD event profile. After you create an event profile, you can apply it to an RPD.

Examples

```
Router(config)>enable
Router#configure terminal
Router(config)#cable profile rpd-event 6
Router(config rpd-event)#priority emergency 0x3
Router(config rpd-event)#priority alert 0x3
Router(config rpd-event)#priority critical 0x3
Router(config rpd-event)#priority error 0x3
Router(config rpd-event)#priority warning 0x3
Router(config rpd-event)#priority notice 0x3
Router(config rpd-event)#priority informational 0x3
Router(config rpd-event)#enable-notify
Router(config)#cable rpd node6
Router(config-rpd)#identifier badb.ad13.5e08
Router(config-rpd)#core-interface Te3/1/5
Router(config-rpd-core)#principal
Router(config-rpd-core)#rpd-ds 0 downstream-cable 3/0/17 profile 10
Router(config-rpd-core)#rpd-us 0 upstream-cable 3/0/34 profile 13
Router(config-rpd-core)#r-dti 16
Router(config-rpd-core)#rpd-event profile 6
```

cable proxy-arp

To activate cable proxy Address Resolution Protocol (ARP) on the cable interface or subinterface, use the **cable proxy-arp** command in cable interface or subinterface configuration mode. To disable this feature, use the **no** form of this command.

cable proxy-arp

no cable proxy-arp

Syntax Description This command has no arguments or keywords.

Command Default Proxy APR service is enabled.

Command Modes Cable interface configuration (config-if)
Cable subinterface configuration (config-subif)

Release	Modification
11.3 XA	This command was introduced.
12.1(3a)EC	The subinterface support was added.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines This command enables or disables direct host-to-host communications over the same cable subnet. Because the downstream and upstream are separate interfaces, CMs cannot directly perform address resolution with other CMs on the cable plant. This means that the CMs must send all traffic through the CMTS, even if the destination CM is on the same subnet.

The **cable proxy-arp** command enables the Cisco CMTS to act as a proxy for ARP requests generated by the CMs, which allows CMs on the same cable subnet to communicate directly with each other, without the traffic having to be routed first through the CMTS. The **no cable proxy-arp** command disables this feature, preventing CMs on the same subnet from communicating with each other without routing the traffic through the CMTS.



Note Using the **no cable arp** and **no cable proxy-arp** commands shifts all responsibility for the management of the IP addresses used by CMs and CPE devices to the DHCP server and provisioning system.

Examples

The following example shows how to activate proxy ARP for host-to-host communications:

```
Router(config-subif)# cable proxy-arp
```

The following example shows how to activate proxy ARP for host-to-host communications, on the cable subinterface:

```
Router(config)# interface cable 6/0.1  
Router(config-subif)# cable proxy-arp
```

Related Commands

Command	Description
cable arp	Activates cable Address Resolution Protocol (ARP).

cable qos enforce-rule

To create an enforce-rule to enforce a particular quality of service (QoS) profile for subscriber traffic management, and to enter enforce-rule configuration mode, use the **cable qos enforce-rule** command in global configuration mode. To delete an enforce-rule and to remove it from the CMTS configuration, use the **no** form of this command.

cable qos enforce-rule *rule-name*

no cable qos enforce-rule *rule-name*

Syntax Description

<i>rule-name</i>	Name of the enforce-rule to be created and configured. This name can be any arbitrary and unique string from 1 to 15 characters in length.
------------------	--

Command Default

No enforce-rules are created.

Command Modes

Global configuration (config)

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. This command replaces the cable qos monitoring command.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.
IOS-XE 3.17.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable qos enforce-rule** command creates an enforce-rule with the specified name and then enters enforce-rule configuration mode. After entering enforce-rule configuration mode, use the following commands to configure the enforce-rule for uBR Series Routers:

- **activate-rule at-byte-count**
- **enabled (enforce-rule)**

- **enforced qos-profile**
- **monitoring-duration**
- **penalty-period**
- **registered qos-profile**

At the very minimum, you must use the **activate-rule at-byte-count** and **registered qos-profile** commands to configure an enforce-rule, and the **enabled** command to activate it, before it takes effect.

**Note**

Effective with Cisco IOS Release 12.3(9a)BC, the **activate-rule at-byte-count** command is not available in Cisco IOS software.

Maximum Number of Rules

The Cisco CMTS routers support a certain maximum number of enforce-rules depending on your Cisco IOS software release. If you have created the maximum number of enforce-rules and want to create another rule, you must first delete one of the existing rules.

- Cisco IOS Release 12.2(15)BC1 and later—Supports a maximum of 20 enforce-rules.
- Beginning in Cisco IOS Release 12.3(23)BC2—Supports a maximum of 40 enforce-rules.
- Cisco IOS Release IOS-XE 3.16.0S and later—Supports a maximum of 40 enforce-rules.

**Note**

The maximum number of enforce-rules is counted as the total number of rules created on both the upstreams and downstreams combined.

Examples

The following example shows the creation of an enforce-rule named “residential.” The system then enters the enforce-rule configuration mode.

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# ?
Configuration commands for QoS enforce rules:
  activate-rule      Activate rule parameters
  enabled            Enable the enforce-rule
  enforced           Enforced qos-profile
  exit              Exit from QoS enforce rule editing mode
  monitoring-duration Monitoring duration parameters
  no                Negate a command or set its defaults
  penalty-period    Penalty-period
  registered         Registered qos-profile
Router(enforce-rule)# activate-rule at-byte-count 5000000 downstream enforced
Router(enforce-rule)# registered qos-profile 5
Router(enforce-rule)# enforced qos-profile 99
Router(enforce-rule)# monitoring-duration 120 sample-rate 20
Router(enforce-rule)# penalty-period 1440
Router(enforce-rule)# enabled
Router(enforce-rule)# exit
Router(config)# exit
```

The following example shows the deletion of an enforce-rule named "test":

```
Router# configure terminal
Router(config)# no cable qos enforce-rule test
```

The following example shows the error message that is displayed if you try to create more than 20 enforce-rules in Cisco IOS Release 12.3(23)BC1 and earlier:

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Can't create more enforce-rules. The maximum number is 20.
```

The following example shows the error message that is displayed when you try to name an enforce-rule with a name that is larger than 15 characters. An error message is displayed, and the name is truncated to the first 15 characters.

```
Router# configure terminal
Router(config)# cable qos enforce-rule reallyreallyreallylongname
Only the first 15 characters would be taken
```

The following example shows the creation of an enforce-rule named "test1" on Cisco cBR Series Converged Broadband Routers. The system then enters the enforce-rule configuration mode.

```
Router(config)#cable qos enforce-rule test1
Router(enforce-rule)# ?
Configuration commands for QoS enforce rules:
  Penalty-period      Penalty period in Minutes
  duration            Legacy monitoring parameters
  enabled             Enable the enforce-rule
  exit               Exit from QoS enforce rule editing mode
  monitoring-basics  Set the monitoring basics
  no                 Negate a command or set its defaults
  peak-time1         Peak-OffPeak parameters
  qos-profile         qos-profile for monitoring cable modems
  service-class      service-class for monitoring cable modems
  weekend             Setup different peak-time for weekends
```

Related Commands

Command	Description
activate-rule at-byte-count	Specifies the number of bytes that a subscriber can transmit during the monitoring period.
debug cable subscriber-monitoring	Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.
enabled (enforce-rule)	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.
duration	Specifies the time period and sample rate to be used for monitoring subscribers.
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.

Command	Description
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.

cable qos permission

To specify permission for updating the quality of service (QoS) table, use the **cable qos permission** command in global configuration mode. To remove a previously enabled permission, use the **no** form of this command.

cable qos permission {**create**| **enforce** *index*| **modems**| **update**}

no cable qos permission

Syntax Description

create	Permits creation of QoS table entries by Simple Network Management Protocol (SNMP).
enforce <i>index</i>	The enforce keyword overrides the provisioned QoS profile of the CM and enforces a specific CMTS-local QoS profile. The <i>index</i> argument specifies the number of the QoS profile to be enforced on all CMs connecting to the CMTS. Valid values are from 1 to 255. Note Both the originally provisioned QoS profile and the enforced QoS profile must be created on the Cisco CMTS. This option does not support profiles that are created by the CM.
modems	Permits creation of QoS table entries by modem registration requests.
update	Permits dynamic update of QoS table entries by SNMP.

Command Default

Enable by modem and SNMP.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3 NA	This command was introduced.
11.3(9)NA	The enforce keyword was added.
12.1(4)CX	This command was deprecated for DOCSIS 1.1 use, because DOCSIS 1.1 replaces the QoS profile model with a service flow model.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

If the QoS profile to be enforced does not exist at the CMTS during registration, the CMTS uses the QoS profile configured for the registering CM.

If you disable the use of CM-created profiles, using the **no cable qos permission** command, any CMs using such a profile go offline immediately and the CM-created profiles are removed.

This **no cable qos permission** command is similar to the docsIfCmtsQosProfilePermissions attribute in the DOCS-IF-MIB, as both prohibit CMs from creating their own QoS profiles in the future. However, the **no cable qos permission** command also immediately deletes QoS profiles that have been created by the cable modems and takes those modems offline. The docsIfCmtsQosProfilePermissions method does not affect QoS profiles that are currently in use, but only unused profiles and profiles that are created in the future.

Examples

The following example shows how to enable CMs to request arbitrary QoS parameters:

```
Router(config)# cable qos permission modems
```

The following example shows how a CM with a QoS profile 4 created by the CM is reset to use QoS profile 225 enforced by the cable router (management):

```
CMTS01# show cable modem
  Interface   SID   Online   Timing Receive QoS IP address   MAC address
           State   Offset Power
Cable6/0/U0  1    online   2848    0.00    4    19.2.20.139   0010.7b6b.7215
CMTS01# show cable qos profile 4
  Service Prio Max      Guarantee Max      Max tx TOS  TOS  Create  B
  class   upstream upstream downstream burst mask value by   priv
           bandwidth bandwidth bandwidth
  4       7    128000    64000    2048000    255  0x0  0x0    cm    no
CMTS01(config)# cable qos profile 225 max-upstream 256
CMTS01(config)# cable qos permission enforce 225
CMTS01# clear cable modem all reset
CMTS01# show cable modem
  Interface   SID   Online   Timing Receive QoS IP address   MACaddress
           State   Offset Power
Cable6/0/U0  1    offline  2848    0.25    2    19.2.20.139   0010.7b6b.7215
CMTS01# debug cable reg
.....
00:15:59: Finished parsing REG Request
00:15:59: Overriding Provisioned QoS Parameters In REG-REQ
.....
CMTS01# show cable modem
  Interface   SID   Online   Timing Receive QoS IP address   MACaddress
           State   Offset Power
Cable6/0/U0  1    online   2852    0.00    225 19.2.20.139   0010.7b6b.7215
CMTS01# show cable qos profile 225
  Service Prio Max      Guarantee Max      Max tx TOS  TOS  Create  B
  class   upstream upstream downstream burst mask value by   priv
           bandwidth bandwidth bandwidth
  225    0    256000    0      0      0    0x0  0x0    management no
```

Related Commands

Command	Description
cable qos profile	Configures a QoS profile.
show cable qos permission	Displays the status of permissions for changing QoS tables for a cable router.

Command	Description
show cable qos profile	Displays the QoS profiles that have been defined.

cable qos pre-registration

To ensure that cable modems get online when a large number of existing online cable modems are actively transmitting data, use the **cable qos pre-registration us-priority** command.

cable qos pre-registration us-priority *priority-value*

Syntax Description

us-priority	Specifies the upstream priority to be assigned to the pre-registration traffic.
<i>priority-value</i>	Priority value of the QoS profile-2. The valid range is from 0 to 7. Note When a cable modem begins initializing, its default upstream service flow is assigned a QoS profile-2 priority of zero. Zero is the lowest priority scheduled.

Command Default

The default QoS profile-2 priority of the initializing cable modem is zero.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCD2	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable qos pre-registration** command allows the Cisco CMTS operators to enforce a profile on all cable modems that have not yet begun initialization. However, this command has no effect on cable modems that have already started initialization and may be having difficulties getting [w-]online.

Examples

The following example shows how to set the priority of the QoS profile-2.

```
Router# configure terminal
Router(config)# cable qos pre-registration us-priority 2
Router(config)#
```

Related Commands

Command	Description
show cable qos profile	Displays the QoS profiles for a Cisco CMTS.

cable qos pro max-ds-burst

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the **cable qos pro max-ds-burst** command in global configuration mode. To remove this ERBA setting from the QoS profile, use the **no** form of this command.

cable qos pro max-ds-burst *burst-size*

no cable qos pro max-ds-burst

Syntax Description

<i>burst-size</i>	The downstream burst size of QoS profile in bytes.
-------------------	--

Command Default

This DOCSIS 1.0 configuration is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(13a)BC	This command was introduced for the Cisco uBR7100 Series and Cisco uB7246VXR router.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

To display ERBA settings as applied to DOCSIS 1.0 cable modems and QoS profiles on the Cisco CMTS, use the **show cable qos profile** command in Privileged EXEC mode.

The following example of the **cable qos profile** command in global configuration mode illustrates changes to the **cable qos profile** command. Fields relating to the ERBA feature are shown in bold for illustration:

```
Router(config)# cable qos pro 10 ?
  grant-interval      Grant interval
  grant-size          Grant size
  guaranteed-upstream  Guaranteed Upstream
  max-burst           Max Upstream Tx Burst
  max-ds-burst       Max Downstream Tx burst (cisco specific)
  max-downstream   Max Downstream
  max-upstream        Max Upstream
  name                QoS Profile name string (cisco specific)

  priority            Priority
  privacy             Cable Baseline Privacy Enable
  tos-overwrite       Overwrite TOS byte by setting mask bits to value
```

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos pro
ID Prio Max Guarantee Max
      TOS TOS Create B IP prec.
      upstream upstream downstream
tx mask value by priv rate
      bandwidth bandwidth bandwidth
burst enab enab
1 0 0 0 0 0
      0 0xFF 0x0 cmts(r) no no
2 0 64000 0 1000000
      0 0xFF 0x0 cmts(r) no no
3 7 31200 31200 0
      0 0xFF 0x0 cmts yes no
4 7 87200 87200 0
      0 0xFF 0x0 cmts yes no
6 1 90000 0 90000
      1522
      0xFF 0x0 mgmt
      yes no
10 1 90000 0 90000
      1522
      0x1 0xA0 mgmt
      no no
50 0 0 0 96000
      0 0xFF 0x0 mgmt no no
51 0 0 0 97000
      0 0xFF 0x0 mgmt no no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos prof verbose** command in privileged EXEC mode:

```
Router# show cable qos pro 10 ver
Profile Index 10
Name
Upstream Traffic Priority 1
Upstream Maximum Rate (bps) 90000
Upstream Guaranteed Rate (bps) 0
Unsolicited Grant Size (bytes) 0
Unsolicited Grant Interval (usecs) 0
Upstream Maximum Transmit Burst (bytes) 1522
Downstream Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask 0x1
IP Type of Service Overwrite Value 0xA0
Downstream Maximum Rate (bps) 90000
Created By mgmt
Baseline Privacy Enabled no
```

If a cable modem registers with a QoS profile that matches one of the existing QoS profiles on the Cisco CMTS, then the maximum downstream burst size, as defined for that profile, is used instead of the default DOCSIS QoS profile of 1522.

For example, a DOCSIS 1.0 configuration that matches QoS profile 10 in the previous examples would be as follows:

```
03 (Net Access Control) = 1
04 (Class of Service Encodings Block)
  S01 (Class ID) = 1
  S02 (Maximum DS rate) = 90000
  S03 (Maximum US rate) = 90000
  S06 (US burst) = 1522
  S04 (US Channel Priority) = 1
  S07 (Privacy Enable) = 0
```

The maximum downstream burst size (as well as the ToS overwrite values) are not explicitly defined in the QoS configuration file because they are not defined in DOCSIS. However, because all other parameters are

a perfect match to profile 10 in this example, then any cable modem that registers with these QoS parameters has a maximum downstream burst of 100000 bytes applied to it.

For further illustration, consider a scenario in which packets are set in lengths of 1000 bytes at 100 packets per second (pps). Therefore, the total rate is a multiplied total of 1000, 100, and 8, or 800kbps.

To change these settings, two or more traffic profiles are defined, with differing downstream QoS settings as desired. The table below provides two examples of such QoS profiles for illustration:

Table 1: Sample QoS Profiles with Differing ERBA (Maximum Downstream) Settings

QoS Profile Setting	QoS Profile 101	QoS Profile 102
Maximum Downstream Transmit Burst (bytes)	max-burst 4000	max-burst 4000
Maximum Downstream Burst (bps)	max-ds-burst 20000	max-ds-burst 5000
Maximum Downstream Bandwidth	max-downstream 100	max-downstream 100

In this scenario, both QoS profiles are identical except for the max-ds-burst size, which is set to 5000 in QoS profile 101 and 5000 in QoS profile 102.

Optimal Settings for DOCSIS 1.0 Downstream Powerburst

DOCSIS allows the setting different token bucket parameters for each service flow, including the token bucket burst size. When burst sizes are closer to 0, QoS is enforced in a stricter manner, allowing a more predictable sharing of network resources, and as a result easier network planning.

When burst sizes are larger, individual flows can transmit information faster (lower latency), although the latency variance can be larger as well.

For individual flows, a larger burst size is likely to be better. As long as the system is not congested, a large burst size reduces the chances of two flows transmitting at the same time, because each burst is likely to take less time to transmit. However, as channel bandwidth consumption increases, it is probably that large burst traffic would exceed the thresholds of buffer depths, and latency is longer than with well shaped traffic.

For additional information about the **cable qos profile** command and configuring QoS profiles, see the *DOCSIS 1.1 for the Cisco CMTS* document on Cisco.com.

Related Commands

Command	Description
cable qos profile	Configures a QoS profile.
show cable qos permission	Displays the status of permissions for changing QoS tables for a cable router.
show cable qos profile	Displays the QoS profiles that have been defined.

cable queue-limit

To set the DOCSIS service flow queue limits to non-default values on the Cisco CMTS, use the **cable queue-limit** command in global configuration mode. To disable this function, use the **no** form of this command.

cable queue-limit *queue_limit_in_ms* **bandwidth-threshold** *threshold_value*

no cable queue-limit *queue_limit_in_ms* **bandwidth-threshold** *threshold_value*

Syntax Description

<i>queue_limit_in_ms</i>	Queue limit in milliseconds. The valid range is from 1 to 200 milliseconds.
<i>threshold_value</i>	Queue bandwidth threshold in Kbps. The valid range is from 0 to 1000000. Note The queue limit specification take effect only if the queue shape rate exceeds the queue-bandwidth threshold.

Command Default

This command is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCG	This command was introduced.
12.2(33)SCG1	Support was added for the Cisco uBR7200 Series router.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable queue-limit bandwidth-threshold** command is used to configure the [DOCSIS WFQ Scheduler on the Cisco CMTS Routers](#) feature.

The queue size on the downstream interfaces can be adjusted to be different than the default settings; for example, when the application can benefit from a larger queue size on a high speed queue.

The queue size in packets is calculated as:

$$\text{queue-size} = \text{bandwidth (Kbps)} * \text{queue-limit (ms)} / 8 / 1518$$

(where 1518 B is the packet size, and bandwidth is the same as queue shape rate).

Examples

The following example shows how to set the queue limit to 25 ms at max-rate when bandwidth exceeds 100000 Kbps:

```
Router(config)# cable queue-limit 25 bandwidth-threshold 100000
```

Related Commands

Command	Description
(For uBR10K Series Routers) show cable modem queue	Displays the queue information on the Cisco uBR7200 router.
(For uBR10K Series Routers) show pxf cpu queue	Displays parallel express forwarding (PXF) queuing, link queue statistics, and the service flow queue information including the queue size on the Cisco uBR10012 router.
(For uBR10K Series Routers) show pxf cable interface	Displays information about a particular service ID (SID), including information about the status of queues used by the SID on the Cisco uBR10012 router.

cable rate-limit-algorithm min-plus-excess

To enable a service flow to receive not only its configured minimum reserved traffic rate bandwidth but also its expected excess traffic rate bandwidth, use the **cable rate-limit-algorithm min-plus-excess** command in global configuration mode. To disable this configuration, use the **no** form of this command.

cable rate-limit-algorithm min-plus-excess

no cable rate-limit-algorithm min-plus-excess

Syntax Description

min-plus-excess	Specifies that the service flow requires a bandwidth of the specified minimum reserved traffic rate, plus excess traffic rate.
------------------------	--

Command Default

When the **cable rate-limit-algorithm min-plus-excess** command is not configured, service flows with the minimum reserved traffic rate configured are guaranteed only their minimum reserved traffic rate. Excess traffic rate bandwidth may not be shared evenly among service flows with or without the minimum rate configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCD5	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Examples

The following example shows how to specify the **min-plus-excess** keyword:

```
Router> enable
Router# configure terminal
Router(config)# cable rate-limit-algorithm argument min-plus-excess
Router(config)#
```

Related Commands

Command	Description
show interface cable mac-scheduler	Displays the current time-slot scheduling state, statistics, and weighted fair queuing (WFQ) parameters for the indicated cable interface.

Command	Description
show interface cable service-flow	Displays the attributes of the DOCSIS service flows on a cable interface.

cable rcc-template

To define a receive channel configuration (RCC) template, use the **cable rcc-template** command in global configuration mode.

cable rcc-template *index*

Syntax Description

<i>index</i>	Specifies an RCC template ID in the range 1 to 255.
--------------	---

Command Default

If an RCC template is not assigned to a cable interface, the CMTS will use the wideband cable interface generated RCC for a receive channel profile (RCP).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
IOS-XE 3.15.0S	This command was replaced by the cable rcc-templates frequency-based command on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

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

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



Note

When assigning an RCC template to a cable interface, use this command in interface configuration mode.

Examples

The following example shows how to define an RCC template:

```
Router# configure terminal
Router(config)# cable rcc-template 1
```

Related Commands

Command	Description
rcp-id	Specifies an ID for the Receive Channel Profile.

Command	Description
receive-module	Specifies a receive module entry in the form of a numeric value.
receive-channel	Specifies a receive channel entry in the form of a numeric value.

cable rcc-templates frequency-based

To allow users to create RCC templates based on frequency-based RCC templates, use the **cable rcc-templates frequency-based** command in global configuration mode. To remove an RCC template, use the **no** form of the command.

cable rcc-templates frequency-based *ID*

no cable rcc-templates frequency-based *ID*

Syntax Description

frequency-based	Specifies frequency-based RCC templates (1 - 8).
<i>ID</i>	RCC template ID. The range is from 1 to 64.

Command Default

Associates an RCC template with a particular MAC domain.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.15.0S	This command was introduced on the Cisco cBR Series Converged Broadband Routers. This command replaces the cable rcc-template command.

Usage Guidelines

This command is used to define multiple RCC templates.

Examples

The following example shows how to define an RCC template:

```
Router(config)# cable rcc-templates frequency-based 1
Router(config-rcc-freq-based)# rcp-id 00 10 18 80 61
(config-rcc-freq-based)# cm-attribute-mask 00ffffff
(config-rcc-freq-based)# rcc-template 1
(config-rcc-freq-based-tmplt)# module 1 channel 1-4 start-frequency 111000000
(config-rcc-freq-based-tmplt)# module 2 channel 5-8 start-frequency 135000000

(config)# interface cable 7/0/0
(config-if)# cable rcc-templates frequency-based 1
```

Related Commands

Command	Description
cable rcp-id	Specifies an ID for the Receive Channel Profile.

cable rcp-control

To enable the receive channel profile (RCP) reporting with verbose description, use the **cable rcp-control** command in interface configuration mode. To revert to the default simple RCP reporting, use the **no** form of this command.

cable rcp-control verbose

no cable rcp-control

Syntax Description

verbose	Enables RCP reporting with verbose description that contains complete subtype encodings defined in DOCSIS 3.0.
----------------	--

Command Default

If this command is not used, cable modems use the default RCP reporting method that contains only the RCP identifiers.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Use this command to enable a CM to send detailed RCP data in the registration request. This detailed RCP data can be verified using the **debug cable registration** command. This verbose RCP data is useful while configuring a receive channel configuration (RCC) template.

Examples

The following example shows how to enable RCP reporting with verbose description on a cable interface on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 8/0/0
Router(config-if)# cable rcp-control verbose
```

The following example shows how to enable RCP reporting with verbose description on a cable interface on the Cisco cBR Series Converged Broadband Routers:

```
Router# configure terminal
```

```
Router(config)# interface cable 3/0/0
Router(config-if)# cable rcp-control verbose
```

Related Commands

Command	Description
debug cable registration	Displays debug messages for the CM registration process.
(For Cisco uBR Series Routers) cable rcc-template	Defines a Receive Channel Configuration (RCC) template.
(For Cisco cBR Series Routers) cable rcc-template frequency-based	Defines a frequency based Receive Channel Configuration (RCC) template.

cable rcp-id

To configure vendor specific Receive Channel Profile's (RCP), use the **cable rcp-id** command in global configuration mode.

cable rcp-id *rcp id*

no cable rcp-id *rcp id*

Syntax Description

<i>rcp id</i>	Specifies a unique RCP ID in hexadecimal.
---------------	---

Command Default

The Standard Receive Channel Profile's (RCP) defined in DOCSIS 3.0 MULPI Specification Annex E are pre-defined in the system by default. These RCP's are un-configurable and can be displayed using the **show cable rcps** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.15.0S	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The RCP's define the physical layer components that permit CM to receive multiple downstream channels. All standard RCP's defined in DOCSIS 3.0 MULPI specification are already pre-loaded into the system. Users can configure vendor specific RCPs using this command.

Examples

The following example shows a typical display for the **cable rcp-id** *rcp id* command for all cable interfaces:

```
Router(config)#cable rcp-id 00 10 18 80 61
Router(config-rcp)#name TI
Router(config-rcp)#center-frequency-spacing 6
Router(config-rcp)#number-of-channels 8
Router(config-rcp)#primary-capable-channels 1
Router(config-rcp)#module 1 minimum-center-frequency 111000000 maximum-center-frequency
999000000
Router(config-rcp)#module 1 number-of-adjacent-channels 10
Router(config-rcp)#module 1 connected-module 1
Router(config-rcp)#module 2 minimum-center-frequency 111000000 maximum-center-frequency
999000000
Router(config-rcp)#module 2 number-of-adjacent-channels 10
Router(config-rcp)#module 2 connected-module 2
#show cable rcp-id 00 10 18 80 61
RCP-ID : 00 10 18 10 61
  Name      : TI
  Number of association      : 1
  Center Frequency Spacing  : 6
  Number of Channels        : 8
  Primary Capable Channels  : 1
  Number of Modules        : 2
```



```
Module [1]:
  Number-of-adjacent-channels : 10
  Minimum-center-frequency    : 111000000
  Maximum-center-frequency    : 999000000
  Connected Module            : 1
Module [2]:
  Number-of-adjacent-channels : 10
  Minimum-center-frequency    : 111000000
  Maximum-center-frequency    : 999000000
  Connected Module            : 2
```

Related Commands

Command	Description
center-frequency-spacing	Specifies center frequency spacing between each channel in RCP.
number-of-channels	Specifies the number of receive channels.

cable reduction-mode energy-management dynamic-channel-percent

To set the percentage of dynamic channel bandwidth, use the **cable reduction-mode energy-management dynamic-channel-percent** command in the global configuration mode. Use the **no** form of the command to restore the default value.

[no] cable reduction-mode energy-management dynamic-channel-percent *value*

Syntax Description

<i>value</i>	Percentage to channel bandwidth when creating dynamic bonding groups for energy management. Valid range is from 1-96.
--------------	---

Command Default

The default value is set to 5.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.18.0S	This command was introduced on Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable reduction-mode energy-management dynamic-channel-percent** command sets the percentage of dynamic channel bandwidth.

Examples

```
Router# configure terminal
Router(config)#cable reduction-mode energy-management dynamic-channel-percent 10
```

cable reduction-mode energy-management enable

To enable the energy management feature, use the **cable reduction-mode energy-management enable** command in the global configuration mode. To disable the energy management feature, use the **no** form of the command.

[no] cable reduction-mode energy-management enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	IOS-XE 3.18.0S	This command was introduced on Cisco cBR Series Converged Broadband Routers.

Usage Guidelines The **cable reduction-mode energy-management enable** command enables the energy management mode.

Examples The following example shows how to enable or disable the energy management feature:

```
Router# configure terminal
Router(config)# cable reduction-mode energy-management enable
Router(config)#no cable reduction-mode energy-management enable
```

Related Commands

Command	Description
show cable modem	Shows if a modem is working in the energy management mode.
Show cable modem reduction-mode energy-management-mode	Shows the the original wideband and upstream channel information.

cablereduction-modeenergy-managementprocess-queue-size

To set the queue size of the energy management requests, use the **cable reduction-mode energy-management process-queue-size** command in the global configuration mode. Use the **no** form of the command to restore the default value.

[no] cable reduction-mode energy-management process-queue-size *value*

Syntax Description

value

Queue size.

Command Default

The default value is set to 150.

Command Modes

Global configuration (config)

Command History

Release

Modification

IOS-XE 3.18.0S

This command was introduced on Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable reduction-mode energy-management process-queue-size** command sets the queue size of the energy management requests.

Examples

```
Router# configure terminal
```

```
Router (config) #cable reduction-mode energy-management process-queue-size 500
```

cable reduction-mode energy-management ranging-init-technique

To configure the technique in init-ranging, use the **cable reduction-mode energy-management ranging-init-technique** command in global configuration mode. Use the **no** form of the command to restore the default value.

[no] **cable reduction-mode energy-management ranging-init-technique** *value*

Syntax Description

<i>value</i>	Value of US init-ranging technique:
	<ul style="list-style-type: none"> • 1—Broadcast • 2—Unicast • 3—Broadcast or unicast • 4—Direct use

Command Default

The default value is set to 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.18.0S	This command was introduced on Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable reduction-mode energy-management ranging-init-technique** command sets the technique in init-ranging.

Examples

```
Router#configure terminal
Router(config)#cable reduction-mode energy-management ranging-init-technique 3
```

cable reduction-mode mta-battery

To configure channel bonding downgrade for cable modems in battery backup mode, use the **cable reduction-mode mta-battery** command in global configuration and interface configuration mode. To remove the configuration, use the **no** form of this command.

```
cable reduction-mode mta-battery { {dampen-time seconds } | {dynamic-channel-percent percent } |
{enable } | { ranging-init-technique us-raning-init-technique } }
```

Syntax Description

dampen-time <i>seconds</i>	Specifies the dampen time in seconds. Valid range is from 30 to 300.
dynamic-channel-percent <i>percent</i>	Specifies the maximum and first try percentage of dynamic channel bandwidth in battery backup mode. Valid range is from 1 to 96.
enable	Enables the channel bonding downgrade for cable modems in battery backup mode.
ranging-init-technique <i>us-raning-init-technique</i>	Specifies the init-ranging technique. The valid values are: <ul style="list-style-type: none"> • 1 - Broadcast. • 2 - Unicast. • 3 - Broadcast or Unicast. • 4 - Direct use.

Command Default

No default behavior or values.

Command Modes

Global configuration (config) and interface configuration (config-if)

Command History

Release	Modification
12.2(33)SCI2	This command was introduced.
IOS-XE 3.16.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Use the **cable reduction-mode mta-battery** command to enable channel bonding downgrade for cable modems in battery backup mode. In addition, you can configure dampen time, init-range technique, maximum and first try percentage using this command.

Examples

The following example shows how to enable the channel bonding downgrade for cable modems in battery backup mode globally:

```
Router(config)# cable reduction-mode mta-battery enable
Router(config)#
```

The following example shows how to configure dampen time:

```
Router(config)# cable reduction-mode mta-battery dampen-time 30
Router(config)#
```

The following example shows how to configure the init-ranging technique:

```
Router(config)# cable reduction-mode mta-battery ranging-init-technique 3
Router(config)#
```

The following example shows how to configure the maximum and first try percentage of dynamic channel bandwidth in battery backup mode:

```
Router(config)# cable reduction-mode mta-battery dynamic-channel-percent 20
Router(config)#
```

The following example shows how to enable the channel bonding downgrade for cable modems in battery backup mode for each MAC domain:

```
Router(config-if)# cable reduction-mode mta-battery enable
Router(config-if)#
```

Related Commands

Command	Description
show cable modem reduction-mode mta-battery	Displays the channel bonding downgrade information for cable modems in battery backup mode.

cable redundancy hashfilter

To set the MAC address and DDC node mappings of the DDC redundancy scheme, use the **cable redundancy hashfilter** command in global configuration mode. This hash filter is to be shared by all DDC nodes (routers) in the redundancy scheme. To remove the hash filter from the Cisco CMTS router, use the **no** form of this command.

cable redundancy hashfilter *hash_id* {**type** *namestring*| **mac-mask** *mac-mask*| **mac-map** *mac-address* **node** *node_id*| **oui-map** *oui* **node** *node_id*}

no cable redundancy hashfilter

Syntax Description

<i>hash_id</i>	Unique ID for the shared hash filter. Multiple (differently named) hash filters are supported in the same Cisco DDC Redundancy scheme at the same time, though only one hash filter can be enabled at any one time. The valid range is from 1 to 3.
type <i>namestring</i>	Alphanumeric hash filter name. Only the namestring of default is supported at this time.
mac-mask <i>mac-mask</i>	Specifies the number of bits in the cable modem's MAC address to be used by the hashing algorithm.
mac-map <i>mac-address</i>	A manually configured MAC address for the DDC node (overrides any default MAC address configured on the router).
node <i>node_id</i>	This value overrides the node that all cable modems with the shared <i>mac-address</i> or <i>oui</i> value will use, and updates the MAC address mapping in the hash filter.
oui-map <i>oui</i>	This value overrides the node that all cable modems with the shared OUI value will use, and updates the OUI address mapping in the hash filter.

Command Default

- Cable redundancy hash filters are disabled (not configured) by default.
- Only the hash filter name of **default** is supported at this time.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This command is used in the early stages of configuring DDC Redundancy on all DDC nodes (routers) in the scheme. For additional information in context, refer to the *Configuring Cisco DDC Redundancy on the Cisco uBR7246VXR Universal Broadband Router* feature documentation on Cisco.com.

**Note**

This configuration must be present and identical on each CMTS router participating in the DDC redundancy scheme.

Examples

The following example implements the **cable redundancy hashfilter** command in four sequential steps, completing the entire mapping information required for one DDC node in a redundancy scheme of two routers:

```
Router# cable redundancy hashfilter 1 type default
Router# cable redundancy hashfilter 1 macmask FFFF.FF00.0000
Router# cable redundancy hashfilter 1 macmap 0007.0e03.68ad node 2
Router# cable redundancy hashfilter 1 ouimap 00070e node 1
```

Related Commands

Command	Description
cable redundancy myid	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
cable redundancy node	Configures the DDC node with active or standby state.
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable redundancy myid

To set the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and to set the ID of the current DDC node, use the **cable redundancy myid** command in global configuration mode. To remove a DDC node ID from the router, use the **no** form of this command.

cable redundancy myid *node_id* **nodes** *nodes*

no cable redundancy myid *node_id*

Syntax Description

<i>node_id</i>	A unique identifier for the Cisco DDC node currently being configured. The value must be 1 or greater (not to exceed the value used for nodes). This value must be unique on each CMTS that participates in the scheme.
<i>nodes</i>	Total number of Cisco CMTS routers participating in the DDC redundancy scheme (range 1 to 3). This value must be identical on all DDC nodes (routers).

Command Default

DDC Redundancy is disabled and DDC nodes (routers) are not configured for DDC redundancy by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This configuration must be present (identical except *node_id*) on all DDC nodes (routers) participating in the scheme.

This command is used in the early stages of configuring DDC Redundancy on all DDC nodes (routers) in the scheme. For additional information in context, refer to the *Configuring Cisco DDC Redundancy on the Cisco uBR7246VXR Universal Broadband Router* feature documentation on Cisco.com.

Examples

The following example configures the DDC node (router) ID to be 2 in a scheme in which there are three DDC nodes total.

```
Router# cable redundancy myid 2 nodes 3
```

Related Commands

Command	Description
cable redundancy node	Configures the DDC node with active or standby state.
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable redundancy node

To set the DDC node (router) with which a subinterface is associated, and to set the state for that interface, use the **cable redundancy node** command in subinterface configuration mode. To remove this configuration from the router, use the **no** form of this command.

cable redundancy node *node_id* {**active**| **standby**} [**force**]

no cable redundancy node *node_id* {**active**| **standby**}

Syntax Description

<i>node_id</i>	DDC node (router) with which the subinterface is associated. The range is the number of DDC nodes in the scheme.
force	Optional keyword forces the subinterface into the standby state regardless of the number of active voice or E911 calls.

Command Default

DDC switchover events are disabled by default and must be manually initiated on a case-by-case basis.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This command can be used in the context of DDC configuration, testing or forced switchover events. Refer to earlier procedures in this document for additional information.



Note

Use of this command is subject to additional constraints described in the *Active Voice Call Protection in Cisco DDC Redundancy* section of the *Configuring Cisco DDC Redundancy on the Cisco uBR7246VXR Universal Broadband Router* feature documentation on Cisco.com.

Examples

The following command sequence sets the DDC node states in a scheme with two DDC nodes (routers), then forces a switchover event on DDC node 1 that puts it into standby state.

```
Router(config-subif)# cable redundancy node 2 active
Router(config-subif)# cable redundancy node 1 standby
Router(config-subif)# cable redundancy node 1 standby force
```

Related Commands

Command	Description
cable redundancy myid	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable redundancy node frequency

To set the downstream frequencies for each node participating in the scheme other than the current DDC node (router), use the **cable redundancy node frequency** command in interface configuration mode. This frequency is used to switch cable modems to the downstream frequency of the backup interface (on another DDC node) via DFO and DCC messages. To remove this setting from the router, use the **no** form of this command.

cable redundancy node *node_id* **frequency** *frequency*

no cable redundancy node *node_id* **frequency** *frequency*

Syntax Description

<i>node_id</i>	DDC target node ID for which the frequency is being set.
<i>frequency</i>	Downstream frequency of the target interface.

Command Default

Cable downstream frequency override is enabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.OS	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This command must be present on each cable interface participating in the scheme, regardless of its bundle status.

Examples

The following example configures the downstream frequency of DDC node 1 to be 435000000.

```
Router(config-if)# cable redundancy node 1 frequency 435000000
```

Related Commands

Command	Description
cable redundancy myid	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.

Command	Description
cable redundancy node	Configures the DDC node with active or standby state.
cable redundancy target	Configures the DDC node by setting the target DDC node (router) to use in a DDC switchover event.
cable redundancy threshold	Configures the DDC node by setting the active voice call threshold on the current DDC node (router)
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable redundancy target

To set the target DDC node (router) to use in a DDC switchover event, use the **cable redundancy target** command in interface configuration mode. To remove this configuration from the router, use the **no** form of this command.

cable redundancy target *node_id*

no cable redundancy target *node_id*

Syntax Description

<i>node_id</i>	Target node ID (in relation to the current DDC node)
----------------	--

Command Default

When this command is not present, the default target node is the next higher node in the scheme.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.OS	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The downstream frequency that is used in a DDC switchover event is the frequency set on the respective target DDC node, as set with this command.



Note

This command may be present on each participating cable interface, regardless of its bundle status.

When this command is not present, the default target node is the next higher node in the scheme (the next higher *node_id* value in the scheme). For example, if there are three participating nodes, the default target nodes are as follows (respectively):

- If the current node is 1, the target node is 2.
- If the current node is 2, the target node is 3.
- If the current node is 3, the target node is 1.

Examples

The following example configures the target node on the current router to be DDC node 1, often referred to as CMTS A in additional sections of this document.

```
Router(config-if)# cable redundancy target 1
```

Related Commands

Command	Description
cable redundancy myid	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
cable redundancy node	Configures the DDC node with active or standby state.
cable redundancy node frequency	Configures the DDC scheme by setting the DS frequencies for each node in the scheme other than the current DDC node (router).
cable redundancy threshold	Configures the DDC node by setting the active voice call threshold on the current DDC node (router).
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable redundancy threshold

To set the active voice call threshold on the current DDC node (router), use the **cable redundancy threshold** command in interface configuration mode. To remove this configuration from the router, use the **no** form of this command.

cable redundancy threshold *max-calls*

no cable redundancy threshold

Syntax Description

<i>max-calls</i>	The threshold value for the number of active voice calls.
------------------	---

Command Default

The threshold for maximum calls is not set by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.
IOS-XE 3.15.OS	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

If the number of active voice calls exceeds this value, a DDC switchover does not take place unless it is forced by using the **cable redundancy node** *node_id* **standby force** subinterface configuration command.

If the command is configured on a bundle master, the threshold is used to compare with the total number of voice calls in the bundle. This command is not accepted on interfaces configured as bundle slaves.

If this threshold is not configured, this check does not occur and the DDC switchover proceeds regardless of how many voice calls are active. This is subject to additional constraints described in the *Call Priority in Cisco DDC Redundancy* section of the *Configuring Cisco DDC Redundancy on the Cisco uBR7246VXR Universal Broadband Router* feature documentation on Cisco.com.

Examples

The following example configures DDC redundancy not to take place if there are more than 20 active or E911 calls at the time a DDC switchover event is attempted or requested.

```
Router(config-if)# cable redundancy threshold 20
```

Related Commands

Command	Description
cable redundancy myid	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
cable redundancy node	Configures the DDC node with active or standby state.
cable redundancy node frequency	Configures the DDC scheme by setting the DS frequencies for each node in the scheme other than the current DDC node (router).
cable redundancy target	Configures the DDC node (node_id) by setting the target DDC node (router) to use in a DDC switchover event.
show cable redundancy	Displays the current DDC redundancy configurations and status.

cable registration-timeout

To set the value of the DOCSIS registration timeout timer (T9 timer) on a particular interface, use the **cable registration-timeout** command in cable interface configuration mode. To reset the timeout value to the default, use the **no** form of this command.

cable registration-timeout *minutes*

no cable registration-timeout

Syntax Description

<i>minutes</i>	Sets the value of the DOCSIS CM registration timeout timer (T9 timer). The range is from 2 to 60. The default is 3.
----------------	---

Command Default

3 minutes

Command Modes

Interface configuration—cable interface only (config-if)

Command History

Release	Modification
12.0(7)XR2	This command was introduced.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The DOCSIS 1.1 specification states that the CMTS should enforce the T9 timer, which is a registration timeout timer that specifies the maximum time allowed between the CMTS sending a successful Ranging Response (RNG-RSP) message and the CM replying with a Registration Request (REG-REQ) message. If this timer expires, the CMTS must remove the CM from its list of active CMs, and the CM must restart the registration process.

The **cable registration-timeout** command can be used to customize the value of the T9 timer for each cable interface, to accommodate the CMs using that interface.

Examples

The following example shows the registration timeout value being increased from 3 minutes to 10 minutes:

```
Router# configure terminal
Router (config)# interface c6/0
Router (config-if)# cable registration-timeout 10
Router (config-if)# exit
Router (config)#
```

cable relay-agent-option

To enable the system to insert the CM MAC address into a Dynamic Host Configuration Protocol (DHCP) packet received from a CM or host and forward the packet to a DHCP server, use the **cable relay-agent-option** command in cable interface configuration mode. To disable MAC address insertion, use the **no** form of this command.

cable relay-agent-option

no cable relay-agent-option

Syntax Description This command has no keywords or arguments.

Command Default MAC address insertion is disabled (**no cable relay-agent-option**).

Command Modes Interface configuration—cable interface only (config-if)

Command History	Release	Modification
	11.3 NA	This command was introduced.
	12.0 mainline, 12.1(2)EC1, 12.0(10) SC	This command was made obsolete and was replaced by the ip dhcp relay information option command.
	IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines This functionality enables the use of DHCP Option 82 to allow a DHCP server to identify the CM sending the request and to initiate the appropriate action based on this information. On Cisco IOS Release 12.0 and later releases, use the **ip dhcp relay information option** command to enable Option 82 processing.

Examples The following example shows how to enable the insertion of DHCP relay agent information into DHCP packets:

```
Router(config-if)# cable relay-agent-option
```

Related Commands

Command	Description
cable helper-address	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast (DHCP) packets.

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

cable resiliency ds-bonding

To enable the Downstream Resiliency Bonding Group feature and to create a resiliency bonding group (RBG) on the Cisco CMTS router, use the **cable resiliency ds-bonding** command in global configuration mode. To disable this feature, use the **no** form of this command.

cable resiliency ds-bonding

no cable resiliency ds-bonding

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SCG	This command was introduced.
	IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines The **cable ds-resiliency** command is used to configure the [Downstream Resiliency Bonding Group](#) feature.

Examples The following example shows how to configure the Downstream Resiliency Bonding Group feature:

```
Router(config)# cable resiliency ds-bonding
```

Related Commands	Command	Description
	cable ds-resiliency	Reserves a resiliency bonding group for a line card on the Cisco CMTS router.
	show cable modem resiliency	Displays resiliency status of the cable modem in resiliency mode on the Cisco CMTS router.
	show cable resiliency	Displays all information about resiliency bonding groups on the Cisco CMTS router.

cable resiliency traps-interval

To set the interval at which traps must be sent for Wideband Resiliency related events for each cable modem on the Cisco CMTS, use the **cable resiliency traps-interval** command in global configuration mode. To disable the interval, use the **no** form of this command.

cable resiliency traps-interval *count*

no cable resiliency traps-interval

Syntax Description

<i>count</i>	Time interval (in seconds) at which the traps must be sent for each cable modem. The range is from 0 to 86400. The default is 1.
--------------	--

Command Default

By default, the resiliency trap interval is enabled and set as 1 second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCG2	This command was introduced.
IOS-XE 3.15.0S	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable resiliency traps-interval** command is associated with the [Wideband Modem Resiliency](#) feature. When the network has less number of cable modems with resiliency events occurring at a given time, use the default value of 1 second interval. But if the network has many cable modems with resiliency events occurring at a given time, set the interval to a higher value.

Examples

The following example shows how to set the time interval to 10 second for sending traps for each cable modem:

```
Router(config)# cable resiliency traps-interval 10
```

Related Commands

Command	Description
show cable modem resiliency	Displays resiliency status of the cable modem in resiliency mode on the Cisco CMTS router.

cable rf-adapt timer

To configure timers for RF adaptation, use the **cable rf-adapt timer** command in global configuration mode. To disable the timers, use the **no** form of this command.

cable rf-adapt timer {*general time*| *candidate time*| *relocation time*}

no cable rf-adapt timer

Syntax Description

general	Period when the RF adaptation process examines the physical layer statistics of all modems on RF adaptation-enabled upstream channels. The valid range is from 1 to 300 seconds. The default value is 10 seconds.
candidate	Period when the RF adaptation process examines the physical layer statistics of modems flagged as downgrade and/or upgrade candidates. The valid range is from 1 to 300 seconds. The default value is 1 second.
relocation	Period when the RF adaptation process performs a single relocation of a candidate modem from its current upstream channel to the appropriate destination. The valid range is from 1 to 300 seconds. The default value is 1 second.
<i>time</i>	Time in seconds. The valid range is from 1 to 300.

Command Default

Default timer values are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCF	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Examples

The following example shows how to set timers for cable modem upstream RF adaptation:

```
Router(config)# cable rf-adapt timer general 120
Router(config)# cable rf-adapt timer candidate 10
Router(config)# cable rf-adapt timer relocation 5
```

Related Commands

Command	Description
cable upstream rf-adapt	Enables RF adaptation on the physical upstream channel.
cable upstream rf-adapt (logical channel)	Configures the primary upstream logical channel and secondary upstream logical channel.
cable upstream threshold	Configures the upstream for the signal-to-noise ratio (SNR) and forward error correction (FEC) threshold values to be used in determining the allowable noise levels.
cable upstream threshold hysteresis	Configures the hysteresis value to be used in conjunction with the dynamic modulation upgrade thresholds.
cable upstream threshold rf-adapt	Configures the upstream RF adaptation threshold value, which prevents excessive relocation of modems from the primary upstream channel to the secondary upstream channel.
show cable modem rf-adapt	Displays the RF adaptation history.
show cable rf-adapt	Displays the downgrade and upgrade candidate lists.

cable rf-bandwidth-percent

To enable either static or dynamic bandwidth sharing for a modular cable (MC) or integrated cable (IC) interface, use the **cable rf-bandwidth-percent** command in interface configuration mode. To remove bandwidth sharing for the MC or IC interface, use the **no** form of this command.

cable rf-bandwidth-percent *percent-value* [**remaining ratio** *excess-value*]

no cable rf-bandwidth-percent

Cisco cBR Series Converged Broadband Routers

cable rf-bandwidth-percent *percent-value*

Syntax Description

<i>percent-value</i>	Specifies static bandwidth allocation of a downstream RF channel. The range is 1–96. The default is 0.
remaining ratio	(Optional) Specifies the ratio of the remaining or excess bandwidth that can be allocated to the modular cable channel. (For Cisco uBR10012 Router and Cisco uBR7200 Series Routers) Note This option is only available when dynamic bandwidth sharing is enabled.
<i>excess-value</i>	(For Cisco uBR10012 Router and Cisco uBR7200 Series Routers) Specifies the value of excess bandwidth that can be allocated to the modular cable channel. The valid range is from 1 to 100. The default is 1.

Command Default

The default static bandwidth percentage for a modular cable or integrated cable interface is 0.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(23)BC	This command was introduced for the Cisco uBR10012 router.
12.3(23)BC1	The remaining ratio option was added.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
IOS-XE 3.15.0S	This command was integrated into Cisco IOS-XE Release 3.15.0S. Support for the Cisco cBR Series Converged Broadband Routers was added.

Usage Guidelines

The total percentage of the RF channel bandwidth allocated to both the modular cable (MC) and wideband interfaces must not exceed 96 percent. The remaining 4 percent of the bandwidth is reserved for minislots allocation packet (MAP) and other MAC management messages (MMM) DOCSIS traffic using this RF channel as its primary channel.

When dynamic bandwidth sharing (DBS) is enabled on the MC or IC interface, the bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding link queue. By re-interpreting the bandwidth percentage value as a CIR value for the interface, the interface receives, at minimum, the configured percent of bandwidth and more when the RF channel's bandwidth is not consumed by other interfaces sharing the same RF channel. The **remaining ratio** option (applicable only for Cisco uBR7K and uBR10K Series Routers) is only available when DBS is enabled using the **cable dynamic-bw-sharing** command.

**Note**

For Cisco cBR Series Converged Broadband Routers, DBS is always enabled but the remaining ratio is not configurable.

(For Cisco uBR7K and uBR10K Series Routers) If the **cable rf-bandwidth-percent** command is not configured and DBS is enabled, no bandwidth is reserved for the MC interface and it is effectively in the protocol down state—the MC link queue is not created. Static bandwidth sharing (the default) or DBS can be configured on an MC interface, but you cannot have both on the same interface.

Examples

The following is an example of static bandwidth allocation configuration:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable rf-bandwidth-percent 70
```

The following is an example of dynamic bandwidth sharing configuration:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# shutdown
Router(config-if)# cable dynamic-bw-sharing
Router(config-if)# no shutdown
Router(config-if)# cable rf-bandwidth-percent 70 remaining ratio 25
```

The following is an example of static bandwidth allocation configuration in cBR Series Converged Broadband Routers:

```
Router# configure terminal
Router(config)# interface Integrated-cable 3/0/0:0
Router(config-if)# cable rf-bandwidth-percent 70
```

Related Commands

Command	Description
cable dynamic-bw-sharing	Enables dynamic bandwidth sharing on a specific modular cable or wideband cable interface.
cable rf-channel	Associates an RF channel on a Wideband SPA with a wideband channel and allocates bandwidth.

Command	Description
show pxf cable controller	Displays information about the RF channel Versatile Traffic Management System (VTMS) links and link queues.
show pxf cpu queue	Displays parallel express forwarding (PXF) queueing and link queue statistics.

cable rf-change-dampen-time

To configure the amount of time a radio frequency (RF) channel must remain in its new state (either up or down), use the **cable rf-change-dampen-time** command in global configuration mode. To restore the default value, use the **no** form of this command.

cable rf-change-dampen-time *seconds*

no cable rf-change-dampen-time

Syntax Description

<i>seconds</i>	Specifies the amount of time in seconds for a non-primary RF channel to remain in its new state. The valid range is 1 to 65535. The default value is 30.
----------------	--

Command Default

If this command is not used, the default value of 30 seconds is restored.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

This command applies to all non-primary RF channels on a CMTS.

Examples

The following example shows how to specify the amount of time for a non-primary RF channel to remain in its new state:

```
Router# configure terminal
Router(config)# cable rf-change-dampen-time 10
```

Related Commands

Command	Description
cable rf-change-trigger	Specifies the persistence thresholds for an event before the event triggers an action for the cable modem.

■ cable rf-change-dampen-time

cable rf-change-trigger

To specify the amount of time an event must persist before it triggers an action for the reporting cable modem, use the **cable rf-change-trigger** command in global configuration mode. To restore the default value, use the **no** form of this command.

cable rf-change-trigger {*percent value*| *count number*} [*secondary*]

no cable rf-change-trigger {*percent value*| *count number*} [*secondary*]

Syntax Description

percent <i>value</i>	Indicates the percentage of cable modems that must report that a particular non-primary RF channel is down before that channel is suspended from the bonding group. The valid range is 1 to 100. The default is 0.
count <i>number</i>	Specifies the number of cable modems that must report that a particular non-primary downstream channel is down before that channel is suspended from the downstream bonding groups. The default is 0.
secondary	(Optional) Configures the Cisco CMTS to move the unicast secondary service flows to the primary channel interface, when the number of cable modems reporting RF channel impairment is less than the configured (percent or count) threshold. By default, the secondary keyword is not configured. Note Only those unicast secondary service flows, which share the same wideband interface as the primary interface, are moved to the primary channel interface.

Command Default

If this command is not used, the default value 0 is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
12.2(33)SCE4	This command was modified. A new keyword secondary was added to move the unicast secondary SFs, which share the same interface as the primary SF, to the primary channel interface when the trigger threshold is not reached.

Release	Modification
IOS-XE 3.15.OS	This command was implemented on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rf-change-trigger** command is used to configure the [Wideband Modem Resiliency](#) feature.

This command applies to all non-primary RF channels on a Cisco CMTS router. The default value of 0 prevents any bonding group modifications. In order to dampen the change of a logical state of an RF channel, the trigger for the channel can be set to one half of the number used for the logical state. For example, if you enter **cable rf-change-trigger percent 20**, when 20 percent of the cable modems report an RF channel is down, the logical state of the RF channel is changed to down. And when 10 percent of the cable modems report that the affected RF channel is back, the logical state is changed to up.

In the case of a small number of wideband modems, you can specify an absolute value for triggering an event in addition to the percentage. Both values must be true in order to trigger the suspension of an RF channel. When both values are 0, the cable modem is reset if the cable modem reports an RF failure through a status message. Also, if you set thresholds to 0, then all cable modems with RF failures are reset and any RFs suspended from a bonding group are reactivated.

Examples

The following example shows how to specify the amount of time an event must persist before it triggers an action for the reporting cable modem:

```
Router# configure terminal
Router(config)# cable rf-change-trigger percent 50 count 1
The following example shows how to configure the Cisco CMTS to move secondary SFs to primary
interface when the trigger threshold is not reached, in Cisco IOS Release 12.2(33)SCE4:
Router# configure terminal
Router(config)# cable rf-change-trigger percent 50 count 1 secondary
```

Related Commands

Command	Description
cable rf-change-dampen-time	Specifies the amount of time an RF channel must remain in its new state.

cable rf-channel

To associate an RF channel on the Cisco Wideband SPA with a wideband interface and allocate bandwidth, use the **cable rf-channel** command in interface configuration mode. To remove an association of an RF channel to a wideband interface, use the **no** form of this command.

cable rf-channel {*rf-port*| **controller** *controller-num* **channel** *channel-num*} [**bandwidth-percent** *bw-percent*] [**remaining ratio** *excess-value*]

no cable rf-channel {*rf-port*| **controller** *controller-num* **channel** *channel-num*}

Syntax Description

<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA field-programmable gate array (FPGA). Note Valid values for the RF <i>port</i> depend on the configuration set with the annex modulation command (see the “Usage Guidelines” section).
<i>controller controller-num</i>	Specifies the controller associated with the RF channel. The valid range is from 0 to 4. Effective with Cisco IOS Release 12.2(33)SCH for Bonding Across 3G60 Controllers Support feature, valid range is from 0 to 2.
<i>channel channel-num</i>	Specifies the channel from the controller. The valid range is from 0 to 3. Effective with Cisco IOS Release 12.2(33)SCH for Bonding Across 3G60 Controllers Support feature, valid range is from 0 to 23.
bandwidth-percent <i>bw-percent</i>	(Optional) Specifies the percent of bandwidth from this RF channel that will be used for the wideband interface. The range is 0 to 100. If bandwidth-percent is not used, the default bandwidth value is 100 percent.
remaining ratio <i>excess-value</i>	(Optional) Specifies the ratio of the excess bandwidth that can be allocated to the wideband interface. The default value is 1. The range is 1 to 100. Note This option is only available when dynamic bandwidth sharing (DBS) is enabled.

Command Default

No default RF channel association with a wideband interface is configured. If the **cable rf-channel** command is used without specifying **bandwidth-percent**, the default bandwidth value is 100 percent.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
12.3(23)BC	The annex and modulation keyword options were added.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.3(23)BC1	The remaining ratio option was added.
12.2(33)SCB	The remaining ratio option was integrated into Cisco IOS Release 12.2(33)SCB.
12.2(33)SCH	The controller option is supported for the Cisco uBR-MC3GX60V cable interface line card on the Cisco uBR10012 router.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rf-channel** command associates an RF channel (port) on a Wideband SPA with a wideband interface. Optionally, you can specify the percent of bandwidth from this RF channel that will be used for the specified wideband interface.

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



Note

The command changes in Cisco IOS releases 12.3(23)BC and 12.3(23)BC1 are not supported in Cisco IOS release 12.2(33)SCA.



Note

In Cisco IOS Releases 12.3(21)BC and 12.3(21a)BC3, the **cable rf-channel** command is not available on the Cisco IOS command line until **annex** and **modulation** have been set with **annex modulation** command. Effective with Cisco IOS Release 12.3(23)BC, the **annex modulation** command is obsolete and **annex** and **modulation** are included as keyword options in the **rf-channel frequency** command.

Each Wideband SPA supports up to 32 wideband channels. A wideband interface cannot consist of RF channels from two different Wideband SPAs. The number of RF channels that can be aggregated into a wideband interface is determined by the capability of the wideband cable modem.

- The Linksys WCM300-NA, WCM300-EURO, and WCM300 JP wideband cable modems can receive a wideband interface consisting of up to eight downstream RF channels at 6 MHz per channel, or up to

six downstream RF channels at 8 MHz per channel. The modem requires that the channels be received in a 50-MHz capture window.

- The Scientific Atlanta DPC2505 and EPC2505 wideband cable modems support the receiving of one wideband interface. The wideband channel consists of three downstream RF channels at either 6 MHz per channel or 8 MHz per channel.

An RF channel can be associated with multiple wideband interfaces as long as the wideband interfaces belong to the same virtual bundle interface (cable bundle) and the RF channel's total allocated bandwidth does not exceed 100 percent. As an example, the table below shows that a single RF channel can be associated with multiple wideband interfaces as long as the total allocated bandwidth for the RF channel does not exceed 100 percent.

Table 2: RF Channel Bandwidth Allocation

RF Channel	Wideband Interface	Bandwidth Allocated
10	0	30 percent
10	1	30 percent
10	2	40 percent
Total Bandwidth Percent: 100 percent		

The table below shows that a single RF channel can be associated with a narrowband and multiple wideband interfaces as long as the total allocated bandwidth for the RF channel does not exceed 100 percent.

Table 3: Bandwidth Allocation Using a Primary-Capable RF Channel

	Modular Cable Interface	Wideband Channel 0	Wideband Channel 1	Wideband Channel 2	Total Bandwidth Percent
Bandwidth Allocated from RF Channel 10	54 percent (4 percent used internally for DOCSIS signaling)	10 percent	22 percent	14 percent	100 percent



Note

Each RF channel on the CMTS can be mapped to a specific QAM port on an edge QAM device. Traffic from different Wideband SPAs cannot be mixed on the same QAM port.

When dynamic bandwidth sharing (DBS) is enabled, the bandwidth percentage is converted to a committed information rate (CIR) value that provides the level of guaranteed bandwidth for the wideband interface. The reserved bandwidth for the wideband interface is the sum of its link queue CIR values and is used for admission control of the service flows with minimal reserved rate. With DBS enabled and the **cable rf-channel** command

configured, the corresponding link queue can have 100 percent of the CIR value. The *excess-value* is the percent of excess bandwidth that can be allocated to the wideband channel.

Static bandwidth sharing (the default) or DBS can be configured on a wideband interface, but you cannot have both on the same interface.

Examples

The following example shows how to associate RF channel 10 and RF channel 11 with wideband interface 0:

```
Router(config)# interface wideband-cable 1/0/0:0
Router(config-if)# cable rf-channel 10 bandwidth-percent 50
```

```
Router(config-if)# cable rf-channel 11
```

The following example shows how to associate a controller to the RF channel for a wideband interface:

```
Router(config)# interface wideband-Cable 7/1/0:0
Router(config-if)# cable rf-channel controller 0 channel 1
```

In the preceding example, because no **bandwidth-percent** is specified in the second **cable rf-channel** command, the default value (100 percent of bandwidth) applies; that is, 100 percent of RF channel 11 bandwidth is used for wideband interface 0.

The following example shows bandwidth allocation when DBS is enabled:

```
Router(config)# interface wideband-cable 1/0/0:0
Router(config-if)# shutdown
Router(config-if)# cable dynamic-bw-sharing
Router(config-if)# no shutdown
Router(config-if)# cable rf-channel 10 bandwidth-percent 50
remaining ratio 5
```

In the preceding example, because DBS is enabled, the wideband interface is guaranteed 50 percent of the bandwidth and 5 as the value for allocating excess bandwidth.

The following example shows how the Bonding Groups Across 3G60 Controllers feature is configured:

```
Router(config-if)#interface wideband-cable 7/0/1:30
Router(config-if)#cable rf-channel controller 1 channel 21 bandwidth-percent 10
Router(config-if)#cable rf-channel controller 1 channel 22 bandwidth-percent 10
Router(config-if)#cable rf-channel controller 1 channel 23 bandwidth-percent 10
Router(config-if)#cable rf-channel controller 0 channel 21 bandwidth-percent 10
Router(config-if)#cable rf-channel controller 0 channel 22 bandwidth-percent 10
Router(config-if)#cable rf-channel controller 0 channel 23 bandwidth-percent 10
Router(config-if)#cable rf-channel 18 bandwidth-percent 10
Router(config-if)#cable rf-channel 19 bandwidth-percent 10
Router(config-if)#end
```

Related Commands

Command	Description
annex modulation	Sets the annex and modulation for the Wideband SPA.
cable bonding-group-id	Specifies a Bonding Group ID and indicates whether the bonding group is a primary or secondary bonded channel.
cable dynamic-bw-sharing	Enables dynamic bandwidth sharing on a specific modular cable or wideband cable interface.

Command	Description
controller modular-cable	Enters controller configuration mode to configure the Wideband SPA controller.
downstream cable	Assigns a primary downstream channel for a fiber node.
ip-address (controller)	Sets the IP address of the Wideband SPA FPGA.
modular-host subslot	Specifies the modular-host line card for Wideband protocol operations.
rf-channel cable downstream channel-id	Assigns a downstream channel ID to an RF channel.
rf-channel description	Specifies the description for each RF channel.
rf-channel frequency	Sets the frequency for each RF channel.
rf-channel ip-address mac-address udp-port	Sets the IP address, MAC address and UDP port for each RF channel.
rf-channel network delay	Specifies the CIN delay for each RF channel.
upstream cable connector	Specifies the upstream channel ports for a fiber node.

cable rf-channels

To associate RF channels on the router with a wideband interface and allocate bandwidth, use the **cable rf-channels** command in interface configuration mode. To remove the association of an RF channel with a wideband interface, use the **no** form of this command.



Note

This command can be used in the wideband interface configuration to specify RF channels on different controllers or to specify different bandwidth percentages.

cable rf-channels [**controller** *controller number*] **channel-list** *group-list* [**bandwidth-percent** *bw-percent*]
no cable rf-channels [**controller** *controller number*] **channel-list** *group-list*

Syntax Description

channel-list <i>group-list</i>	Specifies the channels from the controller. The valid range is from 0 to 127.
controller <i>controller number</i>	(Optional) Specifies the controller associated with the RF channel. The range is from 0 to 7. If not specified, the controller is the same as wideband interface's controller.
bandwidth-percent <i>bandwidth-percent</i>	(Optional) Specifies the percent of bandwidth from this RF channel that is used for the wideband interface. The range is from 0 to 100.

Command Default

RF channel is not associated with a wideband interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS-XE 3.15.0S	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

An RF channel can be associated with multiple wideband interfaces as long as the wideband interfaces belong to the same virtual bundle interface (cable bundle) and the RF channel's total allocated bandwidth does not exceed 100 percent.

An RF channel may be associated to a wideband interface on a different controller using the "controller" option, however the following restriction applies. Wideband interfaces on controllers 0 - 3 may only include RF channels on the same controllers. Likewise, wideband interfaces on controllers 4 - 7 may only include RF channels on those controllers.

Examples

The following example shows how to associate an RF channel with wideband interface and allocate bandwidth:

```
Router(config)# interface Wideband-Cable3/0/0:60
Router(config-if)# cable bundle 1
Router(config-if)# cable rf-channels channel-list 0-1 3-31 bandwidth-percent 1
Router(config)# interface Wideband-Cable3/0/0:45
Router(config-if)# cable bundle 1
Router(config-if)# cable rf-channels controller 2 channel-list 4-6 bandwidth-percent 2
```

cable rswitch copy

To copy an image from the Cisco CMTS router to the Cisco NGRFSW-ADV or from Cisco NGRFSW-ADV to the Cisco CMTS, use the **cable rswitch copy** command in privileged EXEC mode.

cable rswitch copy *filename_cmts* {**to-rfsw**|**from-rfsw**} *filename_rfsw*

Syntax Description

<i>filename_cmts</i>	Filename of the image on or copied to the Cisco CMTS router.
to-rfsw	Copies an image from the Cisco CMTS router to the Cisco NGRFSW-ADV.
from-rfsw	Copies an image from the Cisco NGRFSW-ADV to the Cisco CMTS router.
<i>filename_rfsw</i>	Filename of the image on or copied to the Cisco NGRFSW-ADV.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SCG	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Use the **cable rswitch copy** command when an existing image on the Cisco NGRFSW-ADV or Cisco CMTS router is corrupt or out-of-date and needs to be replaced with another image.

Examples

The following example shows how to download the gcv2.11 image from the Cisco CMTS router to the Cisco NGRFSW-ADV:

```
Router> enable
Router# cable rswitch copy disk0:gcv2.11 to-rfsw gcv2.11
```

The following example shows how to upload the gcv2.11 image from the Cisco NGRFSW-ADV to the Cisco uBR10012 CMTS:

```
Router> enable
Router# cable rfs witch copy disk0:gcv2.11 from-rfsw gcv2.11
```

Related Commands

Command	Description
<code>show hccp channel-switch state</code>	Displays the current state of the Cisco NGRFSW-ADV.

cable rswitch delete

To delete an image in the Cisco NGRFSW-ADV, use the **cable rswitch delete** command in privileged EXEC mode.

cable rswitch delete *filename_rfsw*

Syntax Description

<i>filename_rfsw</i>	Filename of the image on the Cisco NGRFSW-ADV that needs to be deleted.
----------------------	---

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SCG	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rswitch delete** command is used to configure the Cisco uBR Advanced RF Switch (NGRFSW-ADV). For more information, see the [Cisco uBR Advanced RF Switch Software Configuration Guide](#).

Use the **cable rswitch delete** command when an existing image on the Cisco NGRFSW-ADV is corrupt, out-of-date, or needs to be replaced with another image. You cannot delete the active or the golden image on the Cisco NGRFSW-ADV.

Examples

The following example shows how to delete the gcv2.11 image on the Cisco NGRFSW-ADV:

```
Router> enable
Router# cable rswitch delete gcv2.11
```

Related Commands

Command	Description
show hccp channel-switch image	Displays the image list on the Cisco NGRFSW-ADV.
show hccp channel-switch state	Displays the current state of the Cisco NGRFSW-ADV.

cable rfs witch reboot

To reboot the Cisco NGRFSW-ADV, use the **cable rfs witch reboot** command in privileged EXEC mode.

cable rfs witch reboot

Syntax Description

reboot	Reboots the Cisco NGRFSW-ADV.
---------------	-------------------------------

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SCG	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rfs witch reboot** command is used to configure the Cisco uBR Advanced RF Switch (NGRFSW-ADV). For more information, see the [Cisco uBR Advanced RF Switch Software Configuration Guide](#).

Examples

The following example shows how to reboot the Cisco NGRFSW-ADV:

```
Router> enable
Router# cable rfs witch reboot
```

Related Commands

Command	Description
show hccp channel-switch image	Displays the image list on the Cisco NGRFSW-ADV.
show hccp channel-switch state	Displays the current state of the Cisco NGRFSW-ADV.

cable rswitch set-active

To set an image as active on the Cisco NGRFSW-ADV, use the **cable rswitch set-active** command in privileged EXEC mode.

cable rswitch set-active *filename_rfsw*

Syntax Description

<i>filename_rfsw</i>	Filename of the image on the Cisco NGRFSW-ADV that needs to be set as active.
----------------------	---

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SCG	This command was introduced.
IOS-XE 3.15.0S	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rswitch set-active** command is used to configure the Cisco uBR Advanced RF Switch (NGRFSW-ADV). For more information, see the [Cisco uBR Advanced RF Switch Software Configuration Guide](#).

Examples

The following example shows how to set the gcv2.11 image as active on the Cisco NGRFSW-ADV:

```
Router> enable
Router# cable rswitch set-active gcv2.11
Router# cable rswitch reboot
```

Related Commands

Command	Description
show hccp channel-switch image	Displays the image list on the Cisco NGRFSW-ADV.
show hccp channel-switch state	Displays the current state of the Cisco NGRFSW-ADV.

cable rpd

To enter the RPD configuration mode, use the **cable rpd** command in global configuration mode. To void the RPD configuration, use the **no** form of this command.

cable rpd *name*

no cable rpd *name*

Syntax Description

<i>name</i>	Specifies the name of the RPD.
-------------	--------------------------------

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was introduced on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

Use this command to enter the RPD configuration mode.

Examples

The following example shows how to enter the RPD configuration mode:

```
Router# configure terminal
Router(config)# cable rpd
Router(config-rpd)#RphyNode-L01
```

Use this command to apply an Event Profile to RPD.

Examples

The following example shows how to apply an event profile to RPD.

```
Router(config)#cable rpd node6
Router(config-rpd)#identifier badb.ad13.5e08
Router(config-rpd)#core-interface Te3/1/5
Router(config-rpd)#principal
Router(config-rpd)#rpd-ds 0 downstream-cable 3/0/17 profile 10
Router(config-rpd)#rpd-us 0 upstream-cable 3/0/34 profile 13
Router(config-rpd)#r-dti 16
Router(config-rpd)#rpd-event profile 6
```

Use the following command to get events from RPD.

cable rpd {*RPD IP*|*RPD MAC*|*all* }**event**{*locallog*|*pending* }

Related Commands

Command	Description
core-interface	Configures the core-interface of the RPD.
rpd-event profile <i>profile_id</i>	Applies the event profile to RPD.
<i>identifier</i>	MAC address of RPD.
<i>principal</i>	The keyword to specify that this core is the principal core.
<i>rpd-ds 0 downstream-cable downstream_controller profile downstream_controller_profile</i>	Specifies the mapping relationship for RPD downstream channels and the Cisco cBR-8 routers downstream controller.
<i>rpd-us 0 upstream-cable upstream_controller profile upstream_controller_profile</i>	Specifies mapping relationship for RPD upstream port0 and Cisco cBR-8 routers upstream controller.
<i>rpd-us 1 upstream-cable upstream_controller profile upstream_controller_profile</i>	Specifies mapping relationship for RPD upstream port1 and Cisco cBR-8 upstream controller.

cable rsvp default-sc

To specify the default service class that enables the Resource ReSerVation Protocol (RSVP) created service flows to inherit characteristics , use the **cable rsvp default-sc** command in global configuration mode.

cable rsvp default-sc *service-class name*

Syntax Description

<i>service-class name</i>	The name of a downstream DOCSIS service-class .
---------------------------	---

Command Default

Service class is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SCB	This command was introduced.
IOS-XE 3.15.OS	This command is not supported on the Cisco cBR Series Converged Broadband Routers.

Usage Guidelines

The **cable rsvp default-sc** command allows users to specify the default service class that enables the RSVP created service flows to inherit characteristics.

Examples

The following example configures a default RSVP service class.

```
Router# configure terminal
Router(config)# cable service class 220 name RSVPClass
Router(config)# cable service class 220 downstream
Router(config)# cable service class 220 max-latency 100000
Router(config)# cable service class 220 req-attr-mask ffff0000
Router(config)# cable rsvp default-sc RSVPClass
Router(config)# cable rsvp default-sc RSVPClass
```

Related Commands

Command	Description
show cable rsvp flow-db	Displays the contents of the RSVP to DOCSIS service-flow mapping database.