



## Cable Commands: cable p through cable r

---

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

### New Commands

Command	Cisco IOS Software Release
<code>cable rf-bandwidth-percent</code>	12.3(23)BC
<code>cable rcp-control</code>	12.2(33)SCB
<code>cable rcc template</code>	12.2(33)SCB
<code>cable rf-change-dampen-time</code>	12.2(33)SCB
<code>cable rsvp default-scن</code>	12.2(33)SCB
<code>cable rf-change trigger</code>	12.2(33)SCB
<code>cable privacy revocation crl skip-sig-check</code>	12.2(33)SCC
<code>cable privacy revocation enable</code>	12.2(33)SCC
<code>cable privacy revocation oosp skip-sig-check</code>	12.2(33)SCC
<code>cable privacy revocation skip-cm-cert</code>	12.2(33)SCC
<code>cable privacy revocation timeout</code>	12.2(33)SCC

### Modified Commands

Command	Cisco IOS Software Release
<code>cable rf-bandwidth-percent</code>	12.3(23)BC1
<code>cable rf-channel</code>	12.3(23)BC, 12.3(23)BC1
<code>cable rf-bandwidth-percent</code>	12.2(33)SCB
<code>cable rf-channel</code>	12.2(33)SCB

# 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	off	<i>slot/card</i>
	Turns on power to the specified cable interface line card.	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 <b>cable power on</b> version of this command.	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.

## Defaults

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.

## 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
	<b>hw module reset</b>	Resets a line card, performing the equivalent of the <b>shutdown, no shutdown</b> commands.
	<b>show controllers clock-reference</b>	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.
	<b>show interface cable</b>	Displays configuration and status information for a cable interface line card.
	<b>show version</b>	Displays the basic configuration of the router, including whether an active TCC+ card is present.
	<b>shutdown</b>	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

<b>modem</b> <i>mac-addr</i>	Excludes the cable modem with the specified MAC address from pre-equalization during cable modem registration.
<b>oui</b> <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.

## 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# conf t
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 | inc 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 | inc oui
cable pre-equalization exclude oui 00.09.04
```

The following series of commands configures pre-equalization on the Cisco uBR72436VXR router with MC28U cable interface line cards. On the Network Processing Engine (NPE) console, configure and verify with the following commands.

```
Router# conf t
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 | inc 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 | inc 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
<b>debug cable interface</b>	Verifies pre-equalization data and configurations.
<b>debug cable range</b>	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

<b>all</b>	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.
<b>snmp-only</b>	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

## Command History

Release	Modification
12.2(15)CX,	This command was introduced.
12.2(15)BC2	

## 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
<b>cable sflog</b>	Enables service flow logging and configures the number and duration of entries in the log.
<b>show cable modem counters</b>	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.

**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**]

## Syntax Description

<b>accept-self-signed-certificate</b>	(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.
<b>authenticate-modem</b>	(Optional) Uses AAA protocols in conjunction with BPI to authenticate all CMs.
<b>authorize-multicast</b>	(Optional) Uses AAA protocols with baseline privacy interface (BPI) to authorize all multicast stream (IGMP) join requests.
<b>mandatory</b>	(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.
<b>oaep-support</b>	(Optional) Enables Optimal Asymmetric Encryption Padding (OAEP) BPI+ encryption.
<b>dsx-support</b>	(Optional) Enables encryption for dynamic services SIDs.
<b>retain-failed-certificates</b>	(Optional) Allows to retain failed certificates.
<b>skip-validity-period</b>	(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 <b>dsx-support</b> and <b>oaep-support</b> keywords as part of support for BPI+ encryption.
12.2(11)BC1	Changed the <b>accept-self-signed-certificate</b> option from a global configuration option to a cable interface option.

Release	Modification
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 <b>retain-failed-certificates</b> and <b>skip-validity-period</b> keywords. Removed the <b>40-bit-des</b> keyword.

### 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 3/1
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 5/1/1
Router(config-if)# cable privacy authenticate-modem
```

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

```
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 7/1/0
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 3/1
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 3/1
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 3/1
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 3/1
Router(config-if) cable privacy skip-vailidity-period
```

#### Related Commands

Command	Description
<b>cable privacy add-certificate</b>	Adds CM certificates for BPI+ encryption.
<b>cable privacy eae-policy</b>	Selects Early Authentication and Encryption policy.
<b>cable privacy hotlist</b>	Adds a CM certificate to the DOCSIS hotlist so that it is no longer accepted.
<b>cable privacy kek</b>	Sets key encryption keys and timeout periods.
<b>cable privacy tek</b>	Sets traffic encryption keys and timeout periods.
<b>show cable privacy</b>	Displays information about BPI status and operation.
<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# cable privacy add-certificate

To add a manufacturer or root CA certificate to the list of trusted certificates, use the **cable privacy add-certificate** command in global configuration mode. To remove a particular certificate, use the **no** form of this command.

```
cable privacy add-certificate { manufacturer hex-data | root hex-data }
```

```
no cable privacy add-certificate { manufacturer hex-data | root hex-data }
```

## Syntax Description

<b>manufacturer</b> <i>hex-data</i>	Specifies the hexadecimal data for the manufacturer CA certificate. Enter multiple lines as needed, and use a blank line to terminate the string.
<b>root</b> <i>hex-data</i>	Specifies the hexadecimal data for the root CA certificate. Enter multiple lines as needed, and use a blank line to terminate the string.

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.1(7)CX, 12.2(1)XF1, 12.2(4)BC1	This command was introduced.
12.2(11)BC1	The <b>accept-self-signed-certificate</b> option was moved to be part of the <b>cable privacy</b> cable interface command.

## Usage Guidelines

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

## Examples

The following example adds a manufacturer CA certificate to the CMTS list of trusted certificates:

```
Router(config)# cable privacy add-certificate manufacturer  
35c146353431a541463b41337343938333373142  
FEF03A8BC7A441313134749A0A592C9C66831412
```

```
Router(config)#
```

The following example adds a root CA certificate to the CMTS list of trusted certificates:

```
Router(config)# cable privacy add-certificate root 00908300 00300501  
308202A1 3082020A A0030201 02020800 90830000 00000130 0D06092A 864886F7  
0D010105 05003081 92310B30 09060355 04061302 4A503110 300E0603 55040A13  
07546F73 68696261 310F300D 06035504 0B130644 4F435349 53312730 25060355  
040B131E 312D312D 31205368 69626175 7261204D 696E6174 6F2D6B75 20546F6B  
796F3137 30350603 55040313 2E546F73 68696261 20436162 6C65204D 6F64656D  
20526F6F 74204365 72746966 69636174 65204175 74686F72 69747930 1E170D30  
30303331 38303830 3030305A 170D3230 30333138 30383030 30305A30 8192310B
```

## ■ cable privacy add-certificate

```

30090603 55040613 024A5031 10300E06 0355040A 1307546F 73686962 61310F30
0D060355 040B1306 444F4353 49533127 30250603 55040B13 1E312D31 2D312053
68696261 75726120 4D696E61 746F2D6B 7520546F 6B796F31 37303506 03550403

```

```
Router(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
<b>cable privacy hotlist</b>	Adds a CM certificate to the DOCSIS hotlist so that it is no longer accepted.
<b>cable privacy kek</b>	Sets key encryption keys and timeout periods.
<b>cable privacy tek</b>	Sets traffic encryption keys and timeout periods.
<b>option</b>	Determines whether a specific CM is online.
<b>show cable privacy</b>	Displays information about BPI status and operation.
<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# cable privacy bpi-plus-enforce

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**



## Note

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.

## Syntax Description

No additional keywords or arguments

## Command Default

The **cable privacy bpi-plus-enforce** command is not enabled by default, but must be configured for optimal DOCSIS BPI+ security. There is no legitimate reason for a cable modem provisioned with DOCSIS 1.1 QOS to register with DOCSIS 1.0 BPI. Such behavior is not compliant with the DOCSIS 1.1 specification.

## Command Modes

Global configuration mode

## Command History

Release	Modification
12.3(21)BC	This command was introduced to support Cloned Cable Modem Detection for DOCSIS BPI+ on the Cisco uBR10012 and Cisco uBR7246VXR routers.

## Usage Guidelines

If the cable modem is not provisioned to use DOCSIS BPI or BPI+ security certificates, as characterized by not coming online with the above initialization states, then the existing behavior of the Cisco CMTS remains unchanged. The Cisco CMTS does not attempt to distinguish between two cable modems if neither is provisioned for BPI+ security.

Because this feature is enabled by default on the Cisco CMTS, the Cisco CMTS issues security breach notice in a log message in the generic system log or syslog if **cable logging layer2events** is not configured on the Cisco CMTS.

For additional information about the Cable Duplicate MAC Address Reject feature on the Cisco CMTS, or enforced DOCSIS 1.1 security, refer to the following document on Cisco.com:

- *Cable Duplicate MAC Address Reject for the Cisco CMTS*

## Examples

The following brief example illustrates logging messages that are created with the detection of cloned cable modems behind the configuration in the above procedure.

```
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
	<b>cable logging layer2events</b>	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).
	<b>show cable logging</b>	Displays the log of messages about bad IP source addresses or DOCSIS-layer events on the cable interfaces.
	<b>show cable modem</b>	Displays information for registered and non-registered cable modems on the Cisco CMTS.

# 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)

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

**Usage Guidelines** Use this command to enable or disable the clone modem functionality.

**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
	<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
	<b>cable privacy bpi-plus-enforce</b>	Specifies that a cable modem provisioned in DOCSIS 1.1 or higher must register with DOCSIS BPI+, and not use the earlier DOCSIS BPI.
	<b>cable logging layer2events</b>	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).
	<b>show cable logging</b>	Displays the log of messages, about bad IP source addresses or DOCSIS-layer events, on the cable interfaces.
	<b>show cable modem</b>	Displays information for registered and non-registered cable modems on the Cisco CMTS.
	<b>show running-config interface cable</b>	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.

## 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
<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
<b>cable privacy kek</b>	Sets key encryption keys and timeout periods.
<b>cable privacy tek</b>	Sets traffic encryption keys and timeout periods.
<b>show cable privacy</b>	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		
	<b>capability-enforcement</b>	Enforces EAE on capable modems.
	<b>disable-enforcement</b>	Disables EAE thereby preventing the CMTS from enforcing EAE on any cable modem.
	<b>ranging-enforcement</b>	Enforces EAE only on DOCSIS 3.0 modems.
	<b>total-enforcement</b>	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.

**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.

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

```
Router(config)# interface cable 3/1
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 3/1
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 3/1
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 3/1
Router(config-if) cable privacy eae-policy total-enforcement
```

#### Related Commands

Command	Description
<b>cable privacy hotlist</b>	Adds a CM certificate to the DOCSIS hotlist so that it is no longer accepted.
<b>cable privacy kek</b>	Sets Key Encryption Keys and timeout periods.
<b>cable privacy tek</b>	Sets Traffic Encryption Keys and timeout periods.
<b>show cable privacy</b>	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

<b>aes128-des40-des56</b>	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.
<b>aes128-des56-des40</b>	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.
<b>des40-aes128-des56</b>	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.
<b>des40-des56-aes128</b>	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.
<b>des56-aes128-des40</b>	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.
<b>des56-des40-aes128</b>	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.

## Usage Guidelines

Use this command to specify the order of the encryption algorithm priority.

## ■ cable privacy encrypt-alg-priority

### 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
<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
<b>cable privacy kek</b>	Sets Key Encryption Keys and timeout periods.
<b>cable privacy tek</b>	Sets Traffic Encryption Keys and timeout periods.
<b>show cable privacy</b>	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 from registering, use the **cable privacy** 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}
```

## Syntax Description

<b>cm</b> <i>mac-address</i>	Specifies the MAC address for the CM certificate 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.
<b>manufacturer</b> <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.

## Command Default

The CMTS hotlist does not contain any certificates.

## Command Modes

Global configuration

## 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.
12.2(11)BC1	The <b>accept-self-signed-certificate</b> option was moved to the <b>cable privacy</b> cable interface command.
12.2(15)BC2	The <i>mac-address</i> can be specified in the canonical form of three pairs of hexadecimal digits, separated by periods (for example, 0000.0001.0002).

## Usage Guidelines

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. 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](#). For more information see the [Configuring DOCSIS 1.1 on the Cisco CMTS](#) chapter in the [CMTS Feature Guide](#).

## 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# config t
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# config t
Router(config)# cable privacy hotlist manufacturer
3435414631413439383335453731423733333643

Router(config)#
```

### Related Commands

Command	Description
<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
<b>cable privacy add-certificate</b>	Adds CM certificates for BPI+ encryption.
<b>cable privacy kek</b>	Sets key encryption keys and timeout periods.
<b>cable privacy tek</b>	Sets traffic encryption keys and timeout periods.
<b>option</b>	Determines whether a specific CM is online.
<b>show cable privacy</b>	Displays information about BPI status and operation.
<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# cable privacy kek

To set key encryption keys (KEKs) grace-time and 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.

**cable privacy kek life-time** [*seconds*]

**no cable privacy kek life-time**



## Note

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

## Syntax Description

**life-time** *seconds* (Optional) Length of the key encryption life-time in seconds. 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 only (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.

## 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 CM based on the CM service identifier (SID) and permits the CM 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 CM.

A CM that has a grace-time or 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:

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

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

# 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.

## 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
<b>cable privacy revocation oosp skip-sig-check</b>	Allows to skip the OCSP response signature check.
<b>cable privacy revocation skip-cm-cert</b>	Allows to disable checking of the CM certificates.
<b>cable privacy revocation timeout</b>	Sets the timeout value of CRL or OCSP response time.
<b>cable privacy revocation enable</b>	Allows to quickly enable privacy revocation checking.
<b>show cable privacy</b>	Displays information about BPI status and operation.
<b>debug cable privacy</b>	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.

**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
	<b>cable privacy revocation ocsd skip-sig-check</b>	Allows to skip the OCSP response signature check.
	<b>cable privacy revocation skip-cm-cert</b>	Allows to disable checking of the CM certificates.
	<b>cable privacy revocation timeout</b>	Sets the timeout value of CRL or OCSP response time.
	<b>show cable privacy</b>	Displays information about BPI status and operation.
	<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# cable privacy revocation ocsip 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 ocsip skip-sig-check** command in global configuration mode. To enable OCSP signature check, use the **no** form of this command.

**cable privacy revocation ocsip skip-sig-check**

**no cable privacy revocation ocsip 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.

**Usage Guidelines** The **cable privacy revocation ocsip 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 ocsip skip-sig-check
```

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

# 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.

**Usage Guidelines** The **cable privacy revocation skip-cm-cert** command allows you to disable checking of CM certificates.



**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
	<b>cable privacy revocation enable</b>	Allows to quickly enable privacy revocation checking.
	<b>cable privacy revocation ocsip skip-sig-check</b>	Allows to skip the OCSP response signature check.
	<b>cable privacy revocation timeout</b>	Sets the timeout value of CRL or OCSP response time.
	<b>show cable privacy</b>	Displays information about BPI status and operation.
	<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# cable privacy tek

To set traffic encryption keys (TEKs) grace-time and 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.

**cable privacy tek life-time** [*seconds*]

**no cable privacy tek life-time**



## Note

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

## Syntax Description

**life-time** *seconds* (Optional) Length of the traffic encryption life-time in seconds. Valid range is 180 to 604,8000. Default is 43,200 seconds (12 hours).

## Command Default

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

## Command Modes

Interface configuration only (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.

## 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.

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.

A CM that has a grace-time or 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
Router(config-if)# cable privacy tek life-time 800000
Router(config-if)#
```

Related Commands	Command	Description
	<b>cable privacy add-certificate</b>	Configures certificates for BPI+ encryption.
	<b>cable privacy</b>	Enables and configures BPI+ encryption on a cable interface.
	<b>cable privacy kek</b>	Sets key encryption keys and timeout periods.
	<b>option</b>	Determines whether a specific CM is online.
	<b>privacy</b>	Configures the BPI or BPI+ configuration parameters in a DOCSIS configuration file.
	<b>show cable privacy</b>	Displays information about BPI status and operation.
	<b>show interface cable privacy</b>	Displays the current values of the KEK and TEK timers for an interface.
	<b>debug cable privacy</b>	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** Default timeout value is 1 second.

**Command Modes** Global configuration (config)

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

**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
	<b>cable privacy revocation enable</b>	Allows to quickly enable privacy revocation checking.
	<b>cable privacy revocation ocsip skip-sig-check</b>	Allows to skip the OCSP response signature check.
	<b>cable privacy revocation skip-cm-cert</b>	Allows to disable checking of the CM certificates.
	<b>show cable privacy</b>	Displays information about BPI status and operation.
	<b>debug cable privacy</b>	Displays debug messages for BPI operation.

# 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 and subinterface configuration

## Command History

Release	Modification
11.3 XA	This command was introduced.
12.1(3a)EC	The subinterface support was added.

## 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

*rule-name* 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 <b>cable qos monitoring</b> command.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

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:

- **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.



#### 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

Related Commands	Command	Description
	<b>activate-rule at-byte-count</b>	Specifies the number of bytes that a subscriber can transmit during the monitoring period.
	<b>debug cable subscriber-monitoring</b>	Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.
	<b>enabled (enforce-rule)</b>	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.
	<b>duration</b>	Specifies the time period and sample rate to be used for monitoring subscribers.
	<b>penalty-period</b>	Specifies the time period that an enforced QoS profile should be in effect for subscribers that violate their registered QoS profiles.
	<b>qos-profile enforced</b>	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles.
	<b>qos-profile registered</b>	Specifies the registered QoS profile that should be used for this enforce-rule.
	<b>show cable qos enforce-rule</b>	Displays the QoS enforce-rules that are currently defined.
	<b>show cable subscriber-usage</b>	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

<b>create</b>	Permits creation of QoS table entries by Simple Network Management Protocol (SNMP).
<b>enforce</b> <i>index</i>	The <b>enforce</b> 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.
<b>Note</b>	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.
<b>modems</b>	Permits creation of QoS table entries by modem registration requests.
<b>update</b>	Permits dynamic update of QoS table entries by SNMP.

## Command Default

Enable by modem and SNMP

## Command Modes

Global configuration

## Command History

Release	Modification
11.3 NA	This command was introduced.
11.3(9)NA	The <b>enforce</b> 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.

## 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 State	Timing Offset	Receive Power	QoS	IP address	MAC address
Cable6/0/U0	1	online	2848	0.00	4	19.2.20.139	0010.7b6b.7215

```
CMTS01# show cable qos profile 4
```

Service class	Prio	Max upstream bandwidth	Guarantee upstream bandwidth	Max downstream bandwidth	Max tx burst	TOS mask	TOS value	Create by	B priv enab
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 State	Timing Offset	Receive Power	QoS	IP address	MACAddress
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 State	Timing Offset	Receive Power	QoS	IP address	MACAddress
Cable6/0/U0	1	online	2852	0.00	225	19.2.20.139	0010.7b6b.7215

```
CMTS01# show cable qos profile 225
```

Service class	Prio	Max upstream bandwidth	Guarantee upstream bandwidth	Max downstream bandwidth	Max tx burst	TOS mask	TOS value	Create by	B priv enab
225	0	256000	0	0	0	0x0	0x0	management	no

**Related Commands**

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

# cable qos pro max-ds-burst

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the **cable qos promax-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**

<b>Syntax Description</b>	<i>burst-size</i>	The QoS profile's downstream burst size in bytes.
<b>Command Default</b>	This DOCSIS 1.0 configuration is disabled by default.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(13a)BC	This command was introduced for the Cisco uBR7100 Series and Cisco uB7246VXR router.

**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      Max  TOS  TOS  Create  B  IP prec.
      upstream upstream downstream tx   mask value by   priv rate
      bandwidth bandwidth bandwidth burst
1   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	<b>90000</b>	<b>1522</b>	0xFF	0x0	<b>mgmt</b>	yes	no
10	1	90000	0	<b>90000</b>	<b>1522</b>	0x1	0xA0	<b>mgmt</b>	no	no
50	0	0	0	<b>96000</b>	0	0xFF	0x0	mgmt	no	no
51	0	0	0	<b>97000</b>	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
```

## Usage Guidelines

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. [Table 0-8](#) provides two examples of such QoS profiles for illustration:

**Table 0-8 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, refer to the following documents on Cisco.com:

- *DOCSIS 1.1 for the Cisco CMTS*

#### Related Commands

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

## cable qos profile

To configure a QoS profile, use the **cable qos profile** command in global configuration mode. To set a particular value to its default, or to delete the profile when no specific parameters have been set, use the **no** form of this command.

```
cable qos profile groupnum [grant-interval interval | grant-size size | guaranteed-upstream rate
| ip-precedence value | max-burst rate | max-downstream rate | max-upstream rate |
name string | priority value | privacy | tos-overwrite tos-mask tos-value]
```

```
no cable qos profile groupnum [grant-interval interval | grant-size size | guaranteed-upstream
rate | ip-precedence value | max-burst rate | max-downstream rate | max-upstream rate |
name string | priority value | privacy | tos-overwrite]
```

### Syntax Description

<b>groupnum</b> <i>groupnum</i>	QoS profile group number. The valid range is 1 to 255.  QoS profiles 1 and 2 are required by the system; they are preconfigured and cannot be modified nor removed. QoS profile 1 is used during registration; QoS profile 2 is the default QoS profile.
<b>grant-interval</b> <i>interval</i>	The periodic interval in microseconds at which the CM wants to send the fixed-sized upstream MAC frames. It is used to compute the period in between constant bit rate (CBR) slots for the CM. Valid range is from 0 to 65535. The default is 0.
<b>grant-size</b> <i>size</i>	The size of the DOCSIS MAC frame the CM wants periodically to send on the upstream transmission. This value in bytes does not include any PHY layer overhead. It includes the complete fixed MAC frame size starting from the frame control byte to the CRC of the protocol data unit (PDU). This parameter is used by the CMTS to set the size of the periodic CBR slot for the CM after adding the PHY overhead. Valid range is from 0 to 65535. The default is 0.
<b>guaranteed-upstream</b> <i>rate</i>	Guaranteed minimum upstream rate in kilobytes per second. Valid values are from 0 to 100000. Default value is 0 (no reserved rate).
<b>ip-precedence</b> <i>value</i>	Bits in the type-of-service (ToS) byte that enable you to configure individual data rate limits on a per modem basis. Valid values are from 0 to 7. The default is 0.  <b>Note</b> This option has been deprecated and removed from the CLI, because its function should be accomplished through the DOCSIS configuration file.
<b>max-burst</b> <i>rate</i>	Maximum upstream transmit burst size in bytes that the modem can send for any single transmit burst. Valid values are from 0 to 65,535 bytes. Default value is 0 (no limit). The recommended value range is 1600 to 1800 bytes. Using a value of 0 or greater than 1800 bytes can cause latency issues for Voice-over-IP. A value of less than 1500 bytes can prevent the upstream transmission of large Ethernet frames for any modem or CMTS not implementing fragmentation.  <b>Note</b> The CM enforces the maximum upstream transmit burst limit. The Cisco CMTS does not enforce this limit, but this command can still be used for documentation and troubleshooting purposes.

<b>max-downstream</b> <i>rate</i>	Maximum downstream data rate in kilobits per second that a modem using this QoS profile receives. Valid values are from 0 to 100,000. Default value is 0 (no downstream rate limit).  <b>Note</b> This option has been deprecated and removed from the CLI, because its function should be accomplished through the DOCSIS configuration file.
<b>maximum-upstream</b> <i>rate</i>	Maximum upstream data rate in kilobits per second that a modem using this QoS profile receives. Valid values are from 0 to 100,000. Default value is 0 (no upstream rate limit).
<b>name</b> <i>string</i>	Arbitrary, unique string to identify this QoS profile. The maximum length is 32 characters before Cisco IOS Release 12.2(11)BC2, and 80 characters in Cisco IOS Release 12.2(11)BC2 and later.
<b>priority</b> <i>value</i>	Relative priority number assigned to upstream traffic by this QoS profile. Valid values are from 0 to 7, with 7 being the highest priority. Default value is 0.
<b>privacy</b>	Enables Baseline Privacy Interface (BPI) encryption. The default is to disable BPI encryption.
<b>tos-overwrite</b> <i>tos-mask</i> <i>tos-value</i>	Overwrite the ToS field in the IP datagrams received on the upstream before forwarding them downstream (or IP backbone). This parameter sets the hexadecimal mask bits to the hexadecimal values for the ToS mask and ToS value, thereby helping the CMTS identify datagrams for QoS on the backbone.  Each parameter is an 8-bit hexadecimal value that ranges from 0x00 to 0xFF. The default value is 0xFF starting with Cisco IOS Release 12.2(15)BC2 and later, and the default is 0x00 in earlier releases. The new TOS value is calculated using the following formula:  $\text{New ToS} = ((\text{Original ToS}) \text{ AND } (\text{NOT } \textit{tos-mask})) \text{ OR } \textit{tos-value}$  <b>Note</b> This formula is how the TOS was calculated in DOCSIS 1.0+ networks before the DOCSIS 1.1 specification was finalized. For information on the new method of calculating the TOS in DOCSIS 1.1 networks, see the <b>cable service class</b> command.

**Command Default**

If the **cable qos profile** command is given without any options, it creates a profile with all default values: Baseline Privacy Interface is disabled, and all other values are set to 0.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.3 NA	This command was introduced.
12.0(3)T	This command was included in the Release 12.0 T train.
11.3(10)NA and 12.0(4)T	The value for the <i>max-burst</i> parameter was changed from its original value of 0 to 255 minislots (as required in the initial DOCSIS 1.0 specification) to the current, DOCSIS-required value of 0 to 65,535 bytes.

Release	Modification
12.0(5)T	The <b>ip-precedence</b> option was added, and the range for the <b>max-downstream</b> option was increased.
12.0(7)XR2	The output was reorganized and <b>name</b> , <b>grant-size</b> , and <b>grant-interval</b> parameters were 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. See the <b>cable service class</b> command for details.
12.2(11)CY, 12.2(11)BC2	The maximum length of the <b>name</b> string was increased from 32 characters to 80 characters.
12.2(15)BC21	The <b>ip-precedence</b> and <b>max-downstream</b> options were removed, because their functions can be better accomplished through the DOCSIS configuration file.

### Usage Guidelines

The **cable qos profile** command configures the quality of service (QoS) settings for a particular class of service on a DOCSIS 1.0 or DOCSIS 1.0+ network. This command cannot be used on DOCSIS 1.1 and DOCSIS 2.0 networks, which use the **cable service class** command instead.

In Cisco IOS Release 12.2(15)BC21, the **ip-precedence** and **max-downstream** options were removed. If you are supporting DOCSIS 1.0+ CMs that require these parameters for voice over IP (VoIP) traffic and other real-time traffic, use the following Cisco Vendor-Specific Fields (VSIF) in the CM's DOCSIS configuration file:

**Table 9 Cisco VSIF Fields for IP Precedence and Max Downstream Rate**

TLV	Length	Value	Description
10	1	0 to 2	Number of phone lines allowed for the CM.
11	9	1 to 2	IP precedence and maximum downstream rate values, as defined by the following sub-TLVs.
11.1	1	0 to 7	IP precedence value, where 5 is the highest priority (and values 6 and 7 are reserved).
11.2	4	rate in bps	Maximum downstream rate in bits per second (bps), such as 64000 or 256000.

### Examples

The following example shows how to configure QoS profile 4 with a guaranteed upstream rate of 8 kbps, a maximum transmission burst of 1800 bytes, a maximum downstream rate of 128 kbps, a priority of 4, cable baseline privacy set, and a tos-overwrite mask and value byte (in hex) of 0x2:

```
Router(config)# cable qos profile 4 guaranteed-upstream 8
Router(config)# cable qos profile 4 max-burst 1800
Router(config)# cable qos profile 4 max-downstream 128
Router(config)# cable qos profile 4 privacy
Router(config)# cable qos profile 4 priority 4
Router(config)# cable qos profile 4 tos-overwrite 0xE0 0xE0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cable qos permission</b>	Specifies permission for updating the cable router QoS table.
	<b>cable service class</b>	Sets the parameters for DOCSIS 1.1 cable service class.
	<b>show cable qos permission</b>	Displays the status of permissions for changing QoS tables for a cable router.
	<b>show cable qos profile</b>	Displays the QoS profiles that have been defined.

# 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*

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

<b>Command Default</b>	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).	
------------------------	--	--

<b>Command Modes</b>	Global configuration (config)	
----------------------	-------------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SCB	This command was introduced.

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

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



**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>rcp-id</b>	Specifies an ID for the Receive Channel Profile.
	<b>receive-module</b>	Specifies a receive module entry in the form of a numeric value.
	<b>receive-channel</b>	Specifies a receive channel entry in the form of a numeric value.

# 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

<b>verbose</b>	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.

## 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
```

## Related Commands

Command	Description
<b>debug cable registration</b>	Displays debug messages for the CM registration process.
<b>cable rcc-template</b>	Defines a Receive Channel Configuration (RCC) template.

# 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. Supported range is 1 to 3.
<b>type</b> <i>namestring</i>	Alphanumeric hash filter name. Only the namestring of <b>default</b> is supported at this time.
<b>mac-mask</b> <i>mac-mask</i>	Specifies the number of bits in the cable modem's MAC address to be used by the hashing algorithm.
<b>mac-map</b> <i>mac-address</i>	A manually configured MAC address for the DDC node (overrides any default MAC address configured on the router).
<b>node</b> <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.
<b>oui-map</b> <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.

## 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
<b>cable redundancy myid</b>	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
<b>cable redundancy node</b>	Configures the DDC node with active or standby state.
<b>show cable redundancy</b>	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 <i>nodes</i> ). 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.

## 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
<b>cable redundancy node</b>	Configures the DDC node with active or standby state.
<b>show cable redundancy</b>	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.
<b>force</b>	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.

## 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
<b>cable redundancy myid</b>	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
<b>show cable redundancy</b>	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 mode (config-if)

Command History	Release	Modification
	Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.

**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
	<b>cable redundancy myid</b>	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
	<b>cable redundancy node</b>	Configures the DDC node with active or standby state.
	<b>cable redundancy target</b>	Configures the DDC node by setting the target DDC node (router) to use in a DDC switchover event.
	<b>cable redundancy threshold</b>	Configures the DDC node by setting the active voice call threshold on the current DDC node (router)
	<b>show cable redundancy</b>	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.

## 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
<b>cable redundancy myid</b>	Sets the total number of Cisco DDC nodes (routers) in the DDC Redundancy scheme, and sets the ID of the current DDC node.
<b>cable redundancy node</b>	Configures the DDC node with active or standby state.

Command	Description
<b>cable redundancy node frequency</b>	Configures the DDC scheme by setting the DS frequencies for each node in the scheme other than the current DDC node (router).
<b>cable redundancy threshold</b>	Configures the DDC node by setting the active voice call threshold on the current DDC node (router).
<b>show cable redundancy</b>	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**

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

<b>Command Default</b>	The threshold for maximum calls is not set by default.
------------------------	--

<b>Command Modes</b>	Interface configuration (config-if)
----------------------	-------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 12.3(9a)BC	This command was introduced on the Cisco uBR7246 universal broadband router.

<b>Usage Guidelines</b>	If the number of active voice calls exceeds this value, a DDC switchover does not take place unless it is forced by using the <b>cable redundancy node</b> <i>node_id</i> <b>standby force</b> 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.

<b>Examples</b>	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
```

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

---

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

---



---

<b>Command Default</b>	3 minutes
------------------------	-----------

---



---

<b>Command Modes</b>	Interface configuration (cable interface only)
----------------------	--

---



---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(7)XR2	This command was introduced.

---



---

<b>Usage Guidelines</b>	<p>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.</p>
-------------------------	---

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.

---

<b>Examples</b>	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** **no cable relay-agent-option**

**Command Modes** Interface configuration (cable interface only)

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 <b>ip dhcp relay information option</b> command.

**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
	<b>cable helper-address</b>	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast (DHCP) packets.
	<b>cable dhcp-giaddr</b>	Modifies the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address before they are forwarded to the DHCP server.
	<b>cable source-verify</b>	Turns on CM upstream verification.

<b>Command</b>	<b>Description</b>
<b>cable telco-return spd dhcp-authenticate</b>	Enforces the telco-return CM to use a specific DHCP server.
<b>cable telco-return spd dhcp-server</b>	Identifies the IP address of the DHCP server that the telco-return CM must access.
<b>ip dhcp relay information option</b>	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.
<b>ip dhcp smart-relay</b>	Monitors client retransmissions when address pool depletion occurs.

# cable rf-bandwidth-percent

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

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

**no cable rf-bandwidth-percent**

## Syntax Description

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

## Command Default

The default static bandwidth percentage for a modular 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 <b>remaining ratio</b> option was added.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

## 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 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 MC 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 is only available when DBS is enabled using the **cable dynamic-bw-sharing** command.

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
```

**Related Commands**

Command	Description
<b>cable dynamic-bw-sharing</b>	Enables dynamic bandwidth sharing on a specific modular cable or wideband cable interface.
<b>cable rf-channel</b>	Associates an RF channel on a Wideband SPA with a wideband channel and allocates bandwidth.
<b>show pxf cable controller</b>	Displays information about the RF channel Versatile Traffic Management System (VTMS) links and link queues.
<b>show pxf cpu queue</b>	Displays parallel express forwarding (PXF) queueing and link queue statistics.

# cable rf-channel

To associate an RF channel on a 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 [bandwidth-percent bw-percent] [remaining ratio excess-value]
```

```
no cable rf-channel rf-port
```

## Syntax Description

<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA field-programmable gate array (FPGA).  <b>Note</b> Valid values for <i>rf-port</i> depend on the configuration set with the <b>annex modulation</b> command (see the “Usage Guidelines” section).
<b>bandwidth-percent</b> <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 <b>bandwidth-percent</b> is not used, the default bandwidth value is 100 percent.
<b>remaining ratio</b> <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.  <b>Note</b> 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 <b>annex</b> and <b>modulation</b> 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 <b>remaining ratio</b> option was added.
12.2(33)SCB	The <b>remaining ratio</b> option was integrated into Cisco IOS Release 12.2(33)SCB.

## 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, [Table 10](#) 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 10** *RF Channel Bandwidth Allocation*

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

[Table 11](#) 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 11** Bandwidth Allocation Using a Primary-Capable RF Channel

	Modular Cable Interface	Wideband Channel 0	Wideband Channel 1	Wideband Channel 2	Total Bandwidth Percent
<b>Bandwidth Allocated from RF Channel 10</b>	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
```

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.

Related Commands	Command	Description
	<b>annex modulation</b>	Sets the annex and modulation for the Wideband SPA.
	<b>cable bonding-group-id</b>	Specifies a Bonding Group ID and indicates whether the bonding group is a primary or secondary bonded channel.
	<b>cable dynamic-bw-sharing</b>	Enables dynamic bandwidth sharing on a specific modular cable or wideband cable interface.
	<b>controller modular-cable</b>	Enters controller configuration mode to configure the Wideband SPA controller.
	<b>downstream cable</b>	Assigns a primary downstream channel for a fiber node.
	<b>ip-address (controller)</b>	Sets the IP address of the Wideband SPA FPGA.
	<b>modular-host subslot</b>	Specifies the modular-host line card for Wideband protocol operations.
	<b>rf-channel cable downstream channel-id</b>	Assigns a downstream channel ID to an RF channel.
	<b>rf-channel description</b>	Specifies the description for each RF channel.
	<b>rf-channel frequency</b>	Sets the frequency for each RF channel.
	<b>rf-channel ip-address mac-address udp-port</b>	Sets the IP address, MAC address and UDP port for each RF channel.
	<b>rf-channel network delay</b>	Specifies the CIN delay for each RF channel.
	<b>upstream cable connector</b>	Specifies the upstream channel ports for a fiber node.

# 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 will be restored.

**Command Modes** Global configuration (config)

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

**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
	<b>cable rf-change-trigger</b>	Specifies the persistence thresholds for an event before the event triggers an action for the cable modem.

# cable rsvp default-scn

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

**cable rsvp default-scn** *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 mode
---------------	---------------------------

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

Usage Guidelines	The <b>cable rsvp default-scn</b> 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-scn RSVPClass
Router(config)#cable rsvp default-scn RSVPClass
```

Related Commands	Command	Description
	<b>show cable rsvp flow-db</b>	Displays the contents of the RSVP to DOCSIS service-flow mapping database.

# cable rf-change-trigger

To specify the amount of time an event must persist before it triggers an action for the reporting cable modem (CM), 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** *seconds*]

**no cable rf-change-trigger** [**percent** *value*] [**count** *seconds*]

## Syntax Description

<b>percent</b> <i>value</i>	(Optional) Indicates the percentage of cable modems that must report that a particular non-primary RF channel is down before that channel is removed from the bonding group. The valid range is 1 to 100. The default value is 0.
<b>count</b> <i>seconds</i>	(Optional) Specifies the amount of time in seconds. The valid range is 1 to 65535. The default value is 0.

## Command Default

If this command is not used, the default value (0) will be used.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

This command applies to all non-primary RF channels on a CMTS. The default value of 0 will prevent any bonding group modifications. In order to dampen the change of logical state for 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 CMs report an RF channel is down, the RF channel's logical state is changed to down. And when 10 percent of the CMs 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 CM is reset if the CM reports an RF failure through a CM status message. Also, if you set thresholds to 0, then all CMs 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 CM:

```
Router# configure terminal
Router(config)# cable rf-change-trigger percent 50 count 1
```

## ■ cable rf-change-trigger

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



