



# Cable Commands: d through h

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

## New Commands

Command	Cisco IOS Software Release
downstream local upstream	12.3(23)BC
downstream modular-cable rf-channel (interface)	12.3(23)BC
downstream integrated-cable rf-channel (interface)	12.2(33)SCB
depi-class	12.2(33)SCC
depi-tunnel	12.2(33)SCC
dest-ip	12.2(33)SCC
docsis-policy	12.2(33)SCC
docsis-version	12.2(33)SCC
downstream	12.2(33)SCC
depi eqam-stats	12.2(33)SCE
depi cin-failover	12.2(33)SCF
description (bonding-group)	12.2(33)SCG

## Modified Commands

Command	Cisco IOS Software Release
downstream local upstream	12.2(33)SCB
downstream modular-cable rf-channel	12.2(33)SCB
downstream modular-cable rf-channel (interface)	12.2(33)SCB
flowcontrol	12.2(33)SCB
hold-queue	12.2(33)SCB
hw-module bay reload	12.2(33)SCB
duration	12.2(33)SCD2
downstream modular-cable rf-channel (interface)	12.2(33)SCE

**Replaced Commands**

The following commands have been replaced by new commands beginning in the following Cisco IOS software releases:

Command	Replacement Command	Beginning Cisco IOS Release
enforced qos-profile	qos-profile enforced	12.3(9a)BC

# depi cin-failover

To enable a failover when Converged Interconnect Network (CIN) failure occurs on Downstream External PHY Interface (DEPI), use the **depi cin-failover** command in global configuration mode. To disable the failover when the CIN fails on the DEPI, use the **no** form of this command.

**depi cin-failover** [**cpu-threshold** {**high** *threshold\_value* **low** *threshold\_value*}]

**no depi cin-failover**

## Syntax Description

<b>cpu-threshold</b>	Configures the CPU threshold on the line card.
<b>high</b>	Sets the high threshold level. Default value is 95.
<b>low</b>	Sets the low threshold level. Default value is 85.
<i>threshold_value</i>	Threshold value of CPU usage in percentage. The valid range is from 0 to 100.

## Command Default

The DEPI CIN failover configuration is disabled by default.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(33)SCF	This command was introduced.
12.2(33)SCF4	This command was modified. The <b>cpu-threshold</b> keyword was added to the command.

## Usage Guidelines

If DEPI Control Plane High Availability is configured, the **depi cin-failover command**, which is configured globally, triggers a cable line card switchover when a CIN failure occurs.

The **depi cin-failover cpu-threshold** command allows you to set a CPU threshold to alter when a failover due to CIN failure is allowed to happen.

- When the **high** threshold is reached, a failover due to CIN failure is disabled.
- If (and only if) the **high** threshold was reached, the CPU will have to drop lower than the configured **low** threshold before a failover due to CIN failure is enabled again.



### Note

In Cisco IOS Release 12.2(33)SCE, DEPI CIN triggered failover is automatically enabled with control plane DEPI. The **depi cin-failover** command is introduced in Cisco IOS Release 12.2(33)SCF and is disabled by default.

---

**Examples**

The following example shows how to configure a CIN failover:

```
Router(config)# depi  
Router(config)# depi cin-failover  
Router(config)# exit
```

The following example shows how to set the CPU threshold value:

```
Router(config)# depi  
Router(config)# depi cin-failover cpu-threshold high 95 low 85  
Router(config)# exit
```

---

**Related Commands**

Command	Description
<b>show depi tunnel</b>	Displays all active control connections.
<b>show depi session</b>	Displays information about DEPI sessions.

# depi-class

To create a template of Downstream External PHY Interface (DEPI) control plane configuration settings, which different pseudowire classes can inherit, and to enter the DEPI class configuration mode, use the **depi-class** command in global configuration mode. To remove a specific DEPI class configuration, use the **no** form of this command.

**depi-class** *depi-class-name*

**no depi-class** *depi-class-name*

Syntax Description	<i>depi-class-name</i> Name of the DEPI class. The <i>depi-class-name</i> argument must be specified to configure multiple sets of DEPI control parameters.
--------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------

Command Default	No DEPI classes are defined.
-----------------	------------------------------

Command Modes	Global configuration (config)
---------------	-------------------------------

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

Usage Guidelines	<p>The <b>depi-class</b> <i>depi-class-name</i> command allows you to configure a DEPI class template that consists of configuration settings used by different pseudowire classes. The <b>depi-class</b> command enters DEPI class configuration mode, where DEPI control plane parameters are configured.</p> <p>You must use the same DEPI class in the pseudowire configuration at both ends of a Layer 2 control channel.</p>
------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	<p>The following example shows how to enter DEPI class configuration mode to create a DEPI class configuration template for the class named SPA0:</p>
----------	-------------------------------------------------------------------------------------------------------------------------------------------------------

```
Router# configure terminal
Router(config)# depi-class SPA0
Router(config-depi-ctrl SPA0)#
```

Related Commands	Command	Description
	<b>l2tp-class</b>	Creates a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings that can be inherited by different pseudowire classes and enters the L2TP class configuration mode.
	<b>depi-tunnel</b>	Creates a template of Downstream External PHY Interface (DEPI) tunnel configuration settings, which different pseudowire classes can inherit, and enters the DEPI data session configuration mode.

Command	Description
<b>show depi tunnel</b>	Displays all active control connections.
<b>show depi session</b>	Displays established DEPI data sessions.

# depi eqam-stats

To enable debugging information for Downstream External PHY Interface (DEPI) EQAM statistics on the Cisco CMTS router, use the **depi eqam-stats** command in global configuration mode. To disable debugging information, use the **no** form of this command.

**depi eqam-stats**

**no depi eqam-stats**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The DEPI EQAM statistics configuration is enabled by default.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

Cisco RF Gateway 10 sends EQAM statistics to the Cisco CMTS router. No other EQAM supports the EQAM statistics feature.

## Examples

The following example shows how to configure DEPI EQAM statistics on the Cisco CMTS router:

```
Router# configure terminal  
Router(config)# depi eqam-stats
```

## Related Commands

Command	Description
<b>show depi session</b>	Displays information about DEPI sessions.

# depi-tunnel

To create a template of Downstream External PHY Interface (DEPI) tunnel configuration settings, which different pseudowire classes can inherit, and to enter the DEPI data session configuration mode, use the **depi-tunnel** command in the global configuration mode or subinterface configuration mode. To remove a configured DEPI tunnel, use the **no** form of this command.

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

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

## Syntax Description

<i>depi-tunnel-name</i>	Name of the DEPI tunnel.
-------------------------	--------------------------

## Command Default

This command has no default behavior or values.

## Command Modes

Global configuration (config)  
Subinterface configuration (config-subif)

## Command History

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

## Usage Guidelines

The **depi-tunnel** creates a template of DEPI tunnel configuration settings. The DEPI data session inherits the control plane configuration settings of a depi-control template.

The following depi data session configuration options are available in this mode:

- l2tp-class
- depi-class
- dest-ip
- tos

## Examples

The following example shows how to create a template of DEPI tunnel configuration settings in the global configuration mode and enter the DEPI data session configuration mode:

```
Router# configure terminal
Router(config)# depi-tunnel rfc6
Router(config-depi-tunnel)#
```

The following example shows how to create a template of DEPI tunnel configuration settings in the subinterface configuration mode:

```
Router(config)# interface qam 6/4.1
Router(config-subif)# depi-tunnel 0
```



Related Commands	Command	Description
	<b>l2tp-class</b>	Creates a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings, which different pseudowire classes can inherit, and enters the L2TP class configuration mode.
	<b>depi-class</b>	Creates a template of Downstream External PHY Interface (DEPI) control plane configuration settings, which different pseudowire classes can inherit, and enters the DEPI class configuration mode.
	<b>dest-ip</b>	Assigns an IP address to the destination network.
	<b>tos</b>	Configures the Type of Service (ToS) byte in the header of Layer 2 tunneled packets.
	<b>show depi tunnel</b>	Displays all active control connections.
	<b>show depi session</b>	Displays established DEPI data sessions.

# description (bonding-group)

To add a description for a bonding group on the Cisco CMTS router, use the **description** command in cable interface configuration mode. To remove a description for a bonding group, use the **no** form of this command.

**description** *description*

**no description**

Syntax Description	<i>description</i>	Specifies a description for the bonding group. The character-string can be up to 128 characters long.
--------------------	--------------------	-------------------------------------------------------------------------------------------------------

Command Default	By default, description for a bonding group does not exist.
-----------------	-------------------------------------------------------------

Command Modes	Interface configuration (config-if)
---------------	-------------------------------------

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

Usage Guidelines	The <b>description</b> command adds a comment to the configuration to provide information about the bonding group.
------------------	--------------------------------------------------------------------------------------------------------------------

Examples	The following example shows how to specify a description for bonding group 1:
----------	-------------------------------------------------------------------------------

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface cable 8/0/0
Router(config-if)# cable upstream bonding-group 1
Router(config-upstream-bonding)# description UBG1
Router(config-upstream-bonding)# end

Router# show running interface cable 8/0/0

Building configuration...

Current configuration : 1443 bytes
!
interface Cable8/0/0
 downstream Modular-Cable 8/0/0 rf-channel 0-3
 cable ip-init apm
 cable mtc-mode
 no cable packet-cache
 cable bundle 6
 cable upstream max-ports 4
 cable upstream bonding-group 1
```

```
description UBG1
upstream 0
upstream 1
upstream 2
upstream 3
attributes 80000000
```

**Associated Features** The **description** command is used to configure the [Upstream Channel Bonding](#) feature.

Related Commands	Command	Description
	<b>cable fiber-node</b>	Enters cable fiber-node configuration mode to configure a fiber node.
	<b>upstream cable connector</b>	Specifies the upstream channel ports for a fiber node.

# description (cable fiber-node)

To specify a description for a fiber node, use the **description** command in cable fiber-node configuration mode. To remove a description for a fiber node, use the **no** form of this command.

**description** *description*

**no description**

## Syntax Description

<i>description</i>	Specifies a description for the cable fiber node. The character-string can be up to 80 characters long.
--------------------	---------------------------------------------------------------------------------------------------------

## Command Default

If the **description** command is not issued, a description does not exist.

## Command Modes

Cable fiber-node configuration (config-fiber-node)

## Command History

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

## Usage Guidelines

The **description** command adds a comment to the configuration to provide information about the fiber node.

## Examples

The following example shows how to specify a description for fiber node 5:

```
Router# configure terminal
Router(config)# cable fiber-node 5
Router(config-fiber-node)# description Branch office 5
```

## Related Commands

Command	Description
<b>cable fiber-node</b>	Enters cable fiber-node configuration mode to configure a fiber node.
<b>downstream cable</b>	Assigns a primary downstream channel for a fiber node.
<b>downstream modular-cable rf-channel</b>	Specifies the RF channels that are available for wideband channels on a fiber node.
<b>upstream cable connector</b>	Specifies the upstream channel ports for a fiber node.

# dest-ip

To assign an IP address to the edge quadrature amplitude modulation (EQAM), use the **dest-ip** command in DEPI tunnel configuration mode. To remove a specific destination IP address, use the **no** form of this command.

**dest-ip** *dest-ip-address*

**no dest-ip** *dest-ip-address*

<b>Syntax Description</b>	<i>dest-ip-address</i>	IP address of the EQAM.
---------------------------	------------------------	-------------------------

<b>Command Default</b>	This command has no default behavior or values.
------------------------	-------------------------------------------------

<b>Command Modes</b>	DEPI tunnel configuration
----------------------	---------------------------

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

<b>Usage Guidelines</b>	The <b>dest-ip</b> <i>dest-ip-address</i> command allows you to configure the IP address of the EQAM.
-------------------------	-------------------------------------------------------------------------------------------------------

<b>Examples</b>	The following example shows how to assign 1.3.4.155 as the destination IP address:
-----------------	------------------------------------------------------------------------------------

```
Router# configure terminal
Router(config)# depi-tunnel rf6
Router(config-depi-tunnel)# dest-ip 1.3.4.155
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2tp-class</b>	Creates a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings, which different pseudowire classes can inherit, and enters the L2TP class configuration mode.
	<b>depi-class</b>	Creates a template of Downstream External PHY Interface (DEPI) control plane configuration settings, which different pseudowire classes can inherit, and enters the DEPI class configuration mode.
	<b>depi-tunnel</b>	Specifies the name of the depi-tunnel and enters the DEPI tunnel configuration mode.
	<b>tos</b>	Configures the Type of Service (ToS) byte in the header of Layer 2 tunneled packets.
	<b>show depi tunnel</b>	Displays all active control connections.
	<b>show depi session</b>	Displays established DEPI data sessions.

# diagnostic load

To load a Field Diagnostic image to the line card for field diagnostic testing, enter the **diagnostic load** command.

```
diagnostic load {slot slot | subslot slot/subslot} image-url [autostart test {all [port port-number | WORD]} | basic | default | per-port port-number}]
```

Syntax Description	
<b>slot</b>	Specifies that the line card downloading the Field Diagnostic image is in a full slot as opposed to a subslot.
<b>subslot</b>	Specifies that the line card downloading the Field Diagnostic image is in a subslot (in other words, a half-height line card) as opposed to a full slot.
<i>slot</i>	Specifies the number of the slot where the line card downloading the Field Diagnostic image is located on the router.
<i>subslot</i>	Specifies the number of the subslot where the line card downloading the Field Diagnostic image is located on the router.
<i>image-url</i>	Specifies the path where the Field Diagnostic image is being downloaded from. <ul style="list-style-type: none"> <li>If the Field Diagnostic image was saved to the router's Flash file system, enter the file system (such as disk0: or disk1:) as the <i>image-url</i>.</li> <li>If the Field Diagnostic image was saved to a server, the <i>image-url</i> will include <i>server-type://path</i>, where <i>server-type</i> is the type of server (typically either FTP or TFTP) and <i>path</i> is the path to the file on the TFTP server where the Field Diagnostic image has been saved.</li> </ul>
<b>autostart</b>	If <b>autostart</b> is specified, the diagnostic testing process for the line card will begin automatically once the Field Diagnostic image has been loaded onto the line card.
<b>test</b>	The <b>test</b> option is used to specify which type of testing will occur. If the <b>test</b> option is not entered, the default test is used.
<b>all</b>	When used after the <b>test</b> option, specifies that all Field Diagnostic tests will be run during the testing period, including the external loopback test. When used after the <b>port</b> option, specifies that external loopback tests should be run on all ports on the line card.
<b>port</b> <i>port-number</i>	Specifies the port number on the interface that should perform the external loopback test.
<i>WORD</i>	Specifies a range of ports.
<b>basic</b>	Specifies that the basic Field Diagnostic test suite will be run. The basic test suite will catch most hardware problems but not run each individual test like the <b>all</b> test suite option. The advantage of running the basic test suite is that it takes less time to run than the other test suites.
<b>default</b>	Specifies that the default test suite will be run. The default test suite will run all Field Diagnostic tests for the particular line card with the exception of the external loopback test.  If no test suite or test is specified when requesting a test, the default test suite is run.
<b>per-port</b> <i>port-number</i>	Specifies that an external loopback test should be run on a specific port.

**Command Default** If the **autostart** option is entered but no test is specified, the default test suite is the suite used to test the line card.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(16)BX	This command was introduced.
	12.3(13)BC	This command was integrated into Cisco IOS Release 12.3(13)BC.

**Usage Guidelines** Entering this command and successfully downloading the Field Diagnostic image will disrupt normal line card operation. To remove the Field Diagnostic image from a line card and restore normal line card operation, use the **diagnostic unload** command.

If the **autostart** option is not specified, diagnostic tests can be run on the line card after the Field Diagnostic image has been loaded by entering the **diagnostic start** command.

**Examples** In the following example, the **diagnostic load** command is used to download the Field Diagnostic image in TFTP server 127.1.1.1/mytftpfolder to the line card in slot 2. If **yes** is entered at the prompt below, the router will be placed in Field Diagnostic mode.

```
Router# diagnostic load slot 2 tftp://127.1.1.1/mytftpfolder/c10k-fdiagslc-mz.1.1.bin
```

```
*****
WARNING:The specified line card will be taken offline, please ensure that
all traffic has been redirected before executing this command.
```

```
NOTE:The "diagnostic unload <target>" command must be used after diagnostic
testing to resume normal line card operation.
```

```
*****
```

```
Field Diagnostics Image Loading Parameters
```

```
=====
Slot:2 (6oc3pos-1)
Image URL:tftp://127.1.1.1/mytftpfolder/c10k-fdiagslc-mz.1.1.bin
Auto-Start:disabled
=====
```

```
% Are you sure that you want to perform this operation? [no]:
```

Related Commands	Command	Description
	<b>diagnostic event-log size</b>	Sets the size of the event table.
	<b>diagnostic ondemand action-on-failure</b>	Sets the number of errors allowed in the Field Diagnostic test before the Field Diagnostic test is stopped.
	<b>diagnostic ondemand iterations</b>	Sets the number of times each specific Field Diagnostic test will be run when a Field Diagnostic test is initiated.
	<b>diagnostic start</b>	Starts Field Diagnostic testing on the line card.
	<b>diagnostic stop</b>	Stops an in-progress Field Diagnostic test.
	<b>diagnostic unload</b>	Unloads the Field Diagnostic image from the line card and restores normal line card operation.
	<b>show diagnostic content</b>	Shows the Field Diagnostic test list for a particular line card.
	<b>show diagnostic events</b>	Displays the history of Field Diagnostic events since the last system reload.
	<b>show diagnostic ondemand settings</b>	Shows the diagnostic on-demand settings.
	<b>show diagnostic result</b>	Shows the results of the Field Diagnostic test.
	<b>show diagnostic ood-status</b>	Displays various status information, such as line card slot and name, Field Diagnostic image status, and previous Field Diagnostic test results.



# diagnostic ondemand action-on-failure

To set an error count limit or to stop testing once a diagnostic error event is detected, use the **diagnostic ondemand action-on-failure** command.

**diagnostic ondemand action-on-failure** [*continue failure-limit* | **stop**]

## Syntax Description

**continue** *failure-limit*

Specifies that Field Diagnostic testing should continue on the line card after a failed test occurs. The *failure-limit* specifies the number of failed tests that can be detected before testing on the line card should stop. A *failure-limit* of 0 means testing should continue regardless of the number of failed tests.

**Note** The *failure-limit* is the number of failed tests, not errors within a single test. For example, if four errors occur during a single test, the *failure-limit* for that individual test would be 1, not 4.

**stop**

Specifies that Field Diagnostic testing should stop when an error event occurs.

## Command Default

If this command is not entered, a default *failure-limit* of 0 is used. Therefore, testing will continue regardless of the number of errors unless the **diagnostic ondemand action-on-failure** command is used to change the default setting.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(16)BX	This command was introduced.
12.3(13)BC	This command was integrated into Cisco IOS Release 12.2(13)BC.

## Usage Guidelines

The **diagnostic ondemand action-on-failure** settings cannot be saved to a Cisco IOS configuration file. Therefore, the **diagnostic ondemand action-on-failure** command will need to be re-entered each time a router is reset or power cycled if the action-on-failure settings should be maintained.

The **show diagnostic ondemand settings** command can be used to verify the **diagnostic ondemand action-on-failure** setting.

The **show diagnostic events event-type error** command can be used to gather additional information about an error event.

## Examples

In the following example, the diagnostic on-demand iteration and action-on-failure settings are changed using **diagnostic ondemand iterations** and **diagnostic ondemand action-on-failure**. The changed settings are then confirmed using **show diagnostic ondemand settings**.

```
Router# diagnostic ondemand iterations 2
```

```
Router# diagnostic ondemand action-on-failure stop
Router# show diagnostic ondemand settings
```

```
Test iterations = 2
```

**Related Commands<sup>A</sup>**

Command	Description
<b>diagnostic event-log size</b>	Sets the size of the event table.
<b>diagnostic load</b>	Loads the Field Diagnostic image onto the line card.
<b>diagnostic ondemand action-on-failure</b>	Sets the number of errors allowed in the Field Diagnostic test before the Field Diagnostic test is stopped.
<b>diagnostic ondemand iterations</b>	Sets the number of times each specific Field Diagnostic test will be run when a Field Diagnostic test is initiated.
<b>diagnostic start</b>	Starts Field Diagnostic testing on the line card.
<b>diagnostic stop</b>	Stops an in-progress Field Diagnostic test.
<b>show diagnostic content</b>	Shows the Field Diagnostic test list for a particular line card.
<b>show diagnostic events</b>	Displays the history of Field Diagnostic events since the last system reload.
<b>show diagnostic ondemand settings</b>	Shows the diagnostic on-demand settings.
<b>show diagnostic result</b>	Shows the results of the Field Diagnostic test.
<b>show diagnostic ood-status</b>	Displays various status information, such as line card slot and name, Field Diagnostic image status, and previous Field Diagnostic test results.

# diagnostic ondemand iterations

To set the number of times a diagnostic test or set of tests will be run when the **diagnostic start** command is entered, enter the **diagnostic ondemand iterations** command.

**diagnostic ondemand iterations** *iteration-count*

## Syntax Description

*iteration-count*

The number of tests to be run each time a Field Diagnostic test is started. For instance, if the *iteration-count* is set at 2 and the Field Diagnostic test specifies that tests 1, 5, and 10 will be run, tests 1, 5, and 10 will all be run twice. If basic or default testing is specified and the *iteration-count* is 2, all basic or default tests will be run twice.

## Command Default

The default *iteration-count* is 1.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(16)BX	This command was introduced.
12.3(13)BC	This command was integrated into Cisco IOS Release 12.3(13)BC.

## Usage Guidelines

The **diagnostic ondemand iterations** settings cannot be saved to a Cisco IOS configuration file. Therefore, the **diagnostic ondemand iterations** command will need to be re-entered each time a router is reset or power cycled if a nondefault setting needs to be maintained.

The **show diagnostic ondemand settings** command can be used to verify the **diagnostic ondemand iterations** setting.

## Examples

In the following example, the diagnostic on-demand iteration and action-on-failure settings are changed using **diagnostic ondemand iterations** and **diagnostic ondemand action-on-failure**. The changed settings are then confirmed using **show diagnostic ondemand settings**.

```
Router# diagnostic ondemand iterations 2
Router# diagnostic ondemand action-on-failure stop
Router# show diagnostic ondemand settings
```

```
Test iterations = 2
Action on test failure = stop
```

In the following example, the **diagnostic ondemand iterations** command is first used to change the number of iterations per test to 2. Therefore, a Field Diagnostic test is run twice (note that the output of the **diagnostic start** command reflects the test being run twice).

After the initial test, the *iteration-count* is then changed to 3 and the same test is run. Note that the output of **diagnostic start** shows each test being run three times as opposed to two after the *iteration-count* was changed using the **diagnostic ondemand iterations 3** command.

```
Router# diagnostic ondemand iterations 2
Router# diagnostic start slot 8 test 1
Slot 8: Running test(s) 1 may generate packets out of the card interface.

Do you want to run the selected test(s)? [no]: y
Router#

FDIAG [slot 8]> Running Field Diagnostics [Iteration #1] ...
FDIAG [slot 8]> Running MPC860 Register Test {ID=1} ...
FDIAG [slot 8]> MPC860 Register Test {ID=1} passed

FDIAG [slot 8]> Running Field Diagnostics [Iteration #2] ...
FDIAG [slot 8]> Running MPC860 Register Test {ID=1} ...
FDIAG [slot 8]> MPC860 Register Test {ID=1} passed

FDIAG [slot 8]> Total testing time = 00:00:00.500

FDIAG [slot 8]> Field Diagnostics passed with the selected test(s)

*Jun 13 16:05:48.987: %DIAG_C10K-5-TESTING-PASSED: Field Diagnostics passed with the
selected test(s) for card in slot 8
Router# diagnostic ondemand iterations 3
Router# diagnostic start slot 8 test 1
Slot 8: Running test(s) 1 may generate packets out of the card interface.

Do you want to run the selected test(s)? [no]: y
Router#

FDIAG [slot 8]> Running Field Diagnostics [Iteration #1] ...
FDIAG [slot 8]> Running MPC860 Register Test {ID=1} ...
FDIAG [slot 8]> MPC860 Register Test {ID=1} passed

FDIAG [slot 8]> Running Field Diagnostics [Iteration #2] ...
FDIAG [slot 8]> Running MPC860 Register Test {ID=1} ...
FDIAG [slot 8]> MPC860 Register Test {ID=1} passed

FDIAG [slot 8]> Running Field Diagnostics [Iteration #3] ...
FDIAG [slot 8]> Running MPC860 Register Test {ID=1} ...
FDIAG [slot 8]> MPC860 Register Test {ID=1} passed

FDIAG [slot 8]> Total testing time = 00:00:00.600

FDIAG [slot 8]> Field Diagnostics passed with the selected test(s)

*Jun 13 16:06:07.291: %DIAG_C10K-5-TESTING-PASSED: Field Diagnostics passed with the
selected test(s) for card in slot 8
```

## Related Commands<sup>A</sup>

Command	Description
<b>diagnostic event-log size</b>	Sets the size of the event table.
<b>diagnostic load</b>	Loads the Field Diagnostic image onto the line card.
<b>diagnostic ondemand action-on-failure</b>	Sets the number of errors allowed in the Field Diagnostic test before the Field Diagnostic test is stopped.

Command	Description
<b>diagnostic ondemand iterations</b>	Sets the number of times each specific Field Diagnostic test will be run when a Field Diagnostic test is initiated.
<b>diagnostic start</b>	Starts Field Diagnostic testing on the line card.
<b>diagnostic stop</b>	Stops an in-progress Field Diagnostic test.
<b>show diagnostic content</b>	Shows the Field Diagnostic test list for a particular line card.
<b>show diagnostic events</b>	Displays the history of Field Diagnostic events since the last system reload.
<b>show diagnostic ondemand settings</b>	Shows the diagnostic on-demand settings.
<b>show diagnostic result</b>	Shows the results of the Field Diagnostic test.
<b>show diagnostic ood-status</b>	Displays various status information, such as line card slot and name, Field Diagnostic image status, and previous Field Diagnostic test results.

# diagnostic unload

To unload the Field Diagnostic on the line card and resume normal line card operation, enter the **diagnostic unload** command.

**diagnostic unload** {**slot** *slot-number* | **subslot** *slot-number/subslot-number*}

## Syntax Description

<b>slot</b>	Specifies that the line card unloading the Field Diagnostic image is in a full slot as opposed to a subslot.
<b>subslot</b>	Specifies that the line card unloading the Field Diagnostic image is in a subslot as opposed to a full slot.
<i>slot-number</i>	Specifies the number of the slot where the line card unloading the Field Diagnostic image is located on the router.
<i>subslot-number</i>	Specifies the number of the subslot where the line card unloading the Field Diagnostic image is located on the router.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(16)BX	This command was introduced.
12.3(13)BC	This command was integrated into Cisco IOS Release 12.3(13)BC.

## Usage Guidelines

The **show diagnostic result** output will be lost once a Field Diagnostic image is successfully unloaded off a line card. If you want to retain the results of the Field Diagnostic test, enter **show diagnostic result** and copy the output into a separate file before entering **diagnostic unload** to unload the Field Diagnostic image off the line card.

Entering this command successfully will resume normal line card operation.

If a line card needs to be placed back online immediately and a Field Diagnostic test is in progress, enter **diagnostic stop** to stop the in-progress Field Diagnostic test before entering **diagnostic unload** to unload the Field Diagnostic image off the line card.

## Examples

In the following example, the Field Diagnostic image is unloaded off of the line card in slot 2. Note that the command is not successfully executed until confirmed at the screen prompt.

```
Router# diagnostic unload slot 2
```

```
*****
WARNING:All Field Diagnostics test results and information will be
        unavailable to both the "show diagnostic result <target>" and
        "show diagnostic content <target>" commands.
        To save the test results, cancel the unloading process and enter
```

```

the "show diagnostic result <target>" command. Copy the output
into a file, then re-enter the "diagnostic unload <target>" command
to restore normal line card operation.
*****

% Are you sure that you want to perform this operation? [no]:y
FDIAG [slot 2]> Unloading the Field Diagnostics image and restoring the original run-time
image, please wait ...

FDIAG [slot 2]> Field Diagnostics image was successfully unloaded

```

**Related Commands**

Command	Description
<b>diagnostic event-log size</b>	Sets the size of the event table.
<b>diagnostic load</b>	Loads the Field Diagnostic image onto the line card.
<b>diagnostic ondemand action-on-failure</b>	Sets the number of errors allowed in the Field Diagnostic test before the Field Diagnostic test is stopped.
<b>diagnostic ondemand iterations</b>	Sets the number of times each specific Field Diagnostic test will be run when a Field Diagnostic test is initiated.
<b>diagnostic start</b>	Starts Field Diagnostic testing on the line card.
<b>diagnostic stop</b>	Stops an in-progress Field Diagnostic test.
<b>show diagnostic content</b>	Shows the Field Diagnostic test list for a particular line card.
<b>show diagnostic events</b>	Displays the history of Field Diagnostic events since the last system reload.
<b>show diagnostic ondemand settings</b>	Shows the diagnostic on-demand settings.
<b>show diagnostic result</b>	Shows the results of the Field Diagnostic test.
<b>show diagnostic ood-status</b>	Displays various status information, such as line card slot and name, Field Diagnostic image status, and previous Field Diagnostic test results.

## docsis cvc mfg

To configure the access start times and organization name for the manufacturer's code verification certificate (CVC) to enable the DOCSIS 1.1 secure software download feature on the router, use the **docsis cvc mfg** command in global configuration mode. To delete this information, use the **no** form of this command.

**Cisco uBR905 and Cisco uBR925 cable access routers, and Cisco CVA122 Cable Voice Adapter**

**docsis cvc mfg** {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

**no docsis cvc mfg** {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

### Syntax Description

<b>codeAccessStart</b> <i>start-time</i>	Specifies the code Access Start Time as a UTC time value (YYMMDDhhmmssZ) in Greenwich Mean Time.
<b>cvcAccessStart</b> <i>start-time</i>	Specifies the CVC Access Start Time as a UTC time value (YYMMDDhhmmssZ) in Greenwich Mean Time.
<b>organization</b> <i>name</i>	Specifies the name of the manufacturer of the code file. Use quotes if the <i>name</i> value contains more than one word.

### Command Default

The **codeAccessStart** and **cvcAccessStart** times default to 011219000000Z (midnight on December 19, 2001 Greenwich Mean Time). The organization defaults to Cisco Systems.



#### Note

Typically, the default values should not be changed unless you are instructed to do so by Cisco TAC or field service engineers.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

### Usage Guidelines

This command configures the access start times and organization name that are required by Appendix D in the DOCSIS BPI+ specification. The time values are specified as UTC time values in Greenwich Mean Time, with a two-digit year. If the year is between 50 and 99, it is interpreted as 1950 to 1999. If the year is between 00 and 49, it is interpreted as 2000 to 2049.

The router uses the **codeAccessStart** value to verify the Code Verification Signature (CVS) that is affixed to the code file downloaded using the secure software download feature. The router uses the **cvcAccessStart** value to verify the CVC for the code file. The router also uses the **organization** value to verify that the code file has been created by the proper manufacturer.



**Tip**

These values are the same that are set using the docsBpi2CodeMfgCodeAccessStart, docsBpi2CodeMfgCvcAccessStart, and docsBpi2CodeMfgOrgName attributes in the BPI+ MIB (DOCS-BPI2-MIB).

**Examples**

The following example shows the default configuration for the **docsis cvc mfg** commands:

```
Router(config)# docsis cvc mfg organization "Cisco Systems"  
Router(config)# docsis cvc mfg codeAccessStart 011219000000Z  
Router(config)# docsis cvc mfg cvcAccessStart 011219000000Z  
Router(config)#
```

**Note**

You must set the organization name using the **docsis cvc mfg organization** command before you can set either access start time.

**Related Commands**

Command	Description
<b>docsis cvc mso</b>	Configures the access start times and organization name for the optional MSO cosigned code verification certificate (CVC).
<b>docsis cvc test</b>	Tests the root CA public key and CM private key that are installed on the router.

## docsis cvc mso

To configure the access start times and organization name for the optional Multi-Service Operator (MSO) cosigned code verification certificate (CVC) for the DOCSIS 1.1 secure software download feature, use the **docsis cvc mso** command in global configuration mode. To delete the information, use the **no** form of this command.

**Cisco uBR905 and Cisco uBR925 cable access routers, and Cisco CVA122 Cable Voice Adapter**

**docsis cvc mso** {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

**no docsis cvc mso** {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

### Syntax Description

<b>codeAccessStart</b> <i>start-time</i>	Specifies the code Access Start Time as a UTC time value (YYMMDDhhmmssZ) in Greenwich Mean Time.
<b>cvcAccessStart</b> <i>start-time</i>	Specifies the CVC Access Start Time as a UTC time value (YYMMDDhhmmssZ) in Greenwich Mean Time.
<b>organization</b> <i>name</i>	Specifies the name of the manufacturer of the code file. Use quotes if the <i>name</i> value contains more than one word.

### Command Default

No default values or behavior (no cosigner is used).

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

### Usage Guidelines

This command configures the optional cosigner access start times and organization name that are specified by Appendix D in the DOCSIS BPI+ specification. The time values are specified as UTC time values in Greenwich Mean Time, with a two-digit year. If the year is between 50 and 99, it is interpreted as 1950 to 1999. If the year is between 00 and 49, it is interpreted as 2000 to 2049.

You do not need to use this command unless the MSO or service provider is digitally signing the Cisco IOS software images that it plans to download to the Cisco cable modems. If so, then this command must be used to set the appropriate access times and organization name, so that the cable modem can properly authenticate the software images during a secure software download.

The router uses the **codeAccessStart** value to verify the cosigner's Code Verification Signature (CVS) that is affixed to the code file downloaded using the secure software download feature. The router uses the **ccvAccessStart** value to verify the cosigner's CVC that is affixed to the code file. The router also uses the **organization** value to verify that the code file has been signed by the proper MSO or cable operator.

**Tip**

These values are the same that are set using the `docsdocsBpi2CodeCoSignerCodeAccessStart`, `Bpi2CodeCoSignerCvcAccessStart`, and `docsBpi2CodeCoSignerOrgName` attributes in the BPI+ MIB (DOCS-BPI2-MIB).

**Examples**

The following example shows the **docsis cvc mso** commands being used to configure the router for a cosigned CVC from an organization named “MSO Organization” and with certificate access times of midnight on March 1, 2002 Greenwich Mean Time:

```
Router(config)# docsis cvc mfg organization "MSO Organization"
Router(config)# docsis cvc mfg codeAccessStart 020301000000Z
Router(config)# docsis cvc mfg cvcAccessStart 020301000000Z
Router(config)#
```

**Note**

You must set the organization name using the **docsis cvc mso organization** command before you can set either access start time.

**Related Commands**

Command	Description
<b>docsis cvc mfg</b>	Configures the access start times and organization name for the manufacturer’s code verification certificate (CVC).
<b>docsis cvc test</b>	Tests the root CA public key and CM private key that are installed on the router.

# docsis cvc test

To test the root CA public key and CM private key that are installed on the router, use the **docsis cvc test** command in global configuration mode.

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

**docsis cvc test**

**Syntax Description** This command has no arguments or keywords.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

**Usage Guidelines** This command verifies that the root CA public key and the private key that are installed in the router at the factory are valid. The command uses the root CA public key to encrypt a string, and then it uses the router’s private key to decrypt the key.

Typically, the root CA public key and private key are installed at the factory and never need to be updated. However, DOCSIS allows the keys to be updated as part of the secure software download procedure. If this occurs, you can use the **docsis cvc test** command to verify that the keys are valid and are properly installed.

**Examples** The following example shows a typical successful result of the **docsis cvc test** command:

```
Router# config terminal
Router(config)# doctest cvc test
Encrypted sting: This is a test
Encrypt result: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Decrypt result: This is a test
Router(config)#
```



**Note**

If the decrypt result is not “This is a test,” then the test failed, which indicates that either the public key or the private key is not valid.

Related Commands	Command	Description
	<b>docsis cvc mfg</b>	Configures the manufacturer's CVC access start time and organization values.
	<b>docsis cvc mso</b>	Configures the MSO cosigned CVC access start time and organization values.

# docsis-policy

To assign a policy to a DOCSIS load balancing group, use the **docsis-policy** command in the config-lb-group configuration mode. The policy becomes the default policy assigned to the CM, if the CM does not choose a different policy. To remove the assigned policy, use the **no** form of this command.

**docsis-policy** *n*

**no docsis-policy**

<b>Syntax Description</b>	<i>n</i>	Load balancing group policy number. The policy number can range from 0 to 4294967295.
---------------------------	----------	---------------------------------------------------------------------------------------

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	DOCSIS load balancing group mode (config-lb-group)
----------------------	----------------------------------------------------

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

<b>Examples</b>	The following example shows how to assign a policy to a DOCSIS load balancing group on the CMTS, using the <b>docsis-policy</b> command.
-----------------	------------------------------------------------------------------------------------------------------------------------------------------

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# docsis-policy 1
Config: Last Batch 0, 63 bytes
cable load-balance docsis-group 1 index 81
docsis-policy 1
end
```

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

# docsis-version

To configure the DOCSIS version of the CM for the CMTS tag, use the **docsis-version** command in the cmts-tag configuration mode. To remove the configured DOCSIS version from the CMTS tag, use the **no** form of this command.

**[exclude] docsis-version** *docsis-version*

**no docsis-version** *docsis-version*

Syntax Description	exclude	(Optional) Configures the CMTS tag to exclude the specified DOCSIS version.
	<i>docsis-version</i>	DOCSIS version for the CMTS tag. You can select one of the following DOCSIS versions to match the DOCSIS modems: <ul style="list-style-type: none"> <li>docsis10 - Matches DOCSIS 1.0 modems</li> <li>docsis11 - Matches DOCSIS 1.1 modems</li> <li>docsis20 - Matches DOCSIS 2.0 modems</li> <li>docsis30 - Matches DOCSIS 3.0 modems.</li> </ul>

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

**Command Modes** CMTS tag mode (cmts-tag)

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

**Examples** The following example shows how to configure the specified DOCSIS version for the CMTS tag using the **docsis-version** command:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# docsis-version docsis10
```

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

# download

To create a DOCSIS configuration file that instructs the CM to download a new software image, use the **download** command in cable config-file configuration mode. To disable the specification, use the **no** form of this command.

**download** { *image filename* [*oui oui-list*] | *server ip-address* }

**no download** { *image filename* [*oui oui-list*] | *server ip-address* }



## Note

Because of conflicts with other Cisco IOS commands, you cannot abbreviate the **no** form of this command. You must specify the complete command name and option, such as **no download image** or **no download server**.

## Syntax Description

<b>image filename</b>	Specifies to download an image file.
<b>oui oui-list</b>	Specifies the list of Organizational Unique Identifiers (OUIs), up to a maximum of 8. (An OUI is the first 3 octets of the CM MAC address and typically indicates the vendor for the CM.)
<b>Tip</b>	The Institute of Electrical and Electronics Engineers (IEEE) is the official issuer of OUI values. The IEEE OUI web site is at <a href="http://standards.ieee.org/regauth/oui/index.shtml">http://standards.ieee.org/regauth/oui/index.shtml</a> .
<b>server ip-address</b>	Specifies the TFTP server IP address. If no IP address is specified, the CM defaults to using the same TFTP server that provided the configuration file.

## Command Default

The CM does not download a new software image.

## Command Modes

Cable config-file configuration

## Command History

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

## Usage Guidelines

This command sets the Software Upgrade Filename and Software Upgrade TFTP Server fields in the DOCSIS configuration file. The DOCSIS specification allows the DOCSIS configuration file to specify that the CM must be running a particular software image. If the CM is not currently using that image, it must then download the image before continuing the registration process. For security, performance, and scalability reasons, a particular TFTP server can be specified from which the CM must download the new software image.



The *filename* specified by **download image** command must be a fully qualified file and pathname that exactly matches the file and pathname as they exist on the TFTP download server. For example, if the software image is named *ubr920-k1v4y556i-mz* and is in a subdirectory named *cisco\_cms* on the TFTP server, the filename specified with this command should be *cisco\_cms/ubr920-k1v4y556i-mz*.

If the *oui-list* parameter is specified, the **download image** filename is provided only to the CMs that contain those particular OUIs. This helps ensure that the CM does not download a software image that is intended for another vendor's CMs.

**Note**

For each configuration file, multiple download images can be specified. Because each filename can be listed only once, entering a different list of OUIs for a single filename clears the old list. To support more than eight OUIs with the same file, use a different download software image name, and create a duplicate file or alias on the TFTP server.

The **download server** command is not required. If it is not specified, the CM uses the same server that provided its DOCSIS configuration file. However, the **download server** command requires that the image filename also be specified using the **download image** command.

**Examples**

The following command shows how to setup a DOCSIS configuration file so that the cable modem will upgrade its software image:

```
Router(config)# cable config-file upgrade.cm
Router(config-file)# download image ubr920-k1v4y556i-mz.121-3a.T1 oui 00.50.73 00.D0.BA
00.D0.58 00.01.96
Router(config-file)# download server 10.15.24.33
Router(config-file)# exit
Router(config)#
```

**Related Commands**

Command	Description
<b>cable config-file</b>	Creates a DOCSIS configuration file and enters configuration file mode.
<b>access-denied</b>	Disables access to the network.
<b>channel-id</b>	Specifies upstream channel ID.
<b>cpe max</b>	Specifies CPE information.
<b>frequency</b>	Specifies downstream frequency.
<b>option</b>	Provides config-file options.
<b>privacy</b>	Specifies privacy options for baseline privacy images.
<b>service-class</b>	Specifies service class definitions for the configuration file.
<b>snmp manager</b>	Specifies Simple Network Management Protocol (SNMP) options.
<b>timestamp</b>	Enables time-stamp generation.

# downstream

To set downstream radio frequency (RF) channels, use the **downstream** command in the config-lb-group configuration mode. To reset the downstream RF channels, use the **no** form of this command.

## Cisco uBR7200 Series Routers

**downstream cable** {slot/port}

**no downstream cable** {slot/port}

## Cisco uBR10012 Router

**downstream** {cable {slot/subslot/port} | **Integrated-Cable** {slot/subslot/bay} {rf-channel group list} | **Modular-Cable** {slot/subslot/bay} {rf-channel group list}}

**no downstream** {cable {slot/subslot/port} | **Integrated-Cable** {slot/subslot/bay} {rf-channel group list} | **Modular-Cable** {slot/subslot/bay} {rf-channel group list}}

Syntax Description		
<b>cable</b> {slot/port}		Specifies the CMTS interface slot and port numbers.
<b>cable</b> {slot/subslot/port}		Specifies the CMTS interface slot, subslot, and port numbers.
<b>Integrated-Cable</b> {rf-channel group list} {slot/subslot/bay}		Specifies the integrated cable interface with the list of port numbers that range in the associated RF channel. Slot, subslot, and bay numbers of the integrated cable interface is also specified.
<b>Modular-Cable</b> {rf-channel group list} {slot/subslot/bay}		Specifies the modular cable interface with the list of port numbers that range in the associated RF channel. It also specifies slot, subslot, and bay numbers of the modular cable interface.

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

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

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

**Examples** The following example shows how to set downstream RF channels to a DOCSIS load balancing group on the CMTS, using the **downstream** command.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# downstream cable 1/1
Router(config-lb-group)# downstream Integrated-Cable 5/0/0 rf-channel 2
Router(config-lb-group)# downstream Modular-Cable 1/0/0 rf-channel 4
```

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

# downstream cable

To assign a primary downstream channel for a fiber node, use the **downstream cable** command in cable fiber-node configuration mode. To remove a primary downstream channel for a fiber node, use the **no** form of the command.

**downstream cable** *slot/subslot/port*

**no downstream cable** *slot/subslot/port*

## Syntax Description

<i>slot</i>	The slot used for the cable interface line card. Valid values are 5 to 8.
<i>subslot</i>	The subslot used for the cable interface line card. Valid values are 0 or 1.
<i>port</i>	The downstream port that can be used as a primary downstream channel. Valid values are 0 to 4.

## Command Default

If the **downstream cable** command is not issued, no primary downstream channel is assigned to the fiber node.

## Command Modes

Cable fiber-node configuration

## Command History

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

## Usage Guidelines

For each fiber node, a traditional DOCSIS downstream channel is used to carry MAC management and signaling messages, and the associated traditional DOCSIS upstream channel is used for return data traffic and signaling. The traditional DOCSIS downstream channel used in this way is called the *primary downstream channel*.

The **downstream cable** command assigns a primary downstream channel for a fiber node. Each fiber node must be assigned at least one primary downstream channel and can be assigned multiple primary downstream channels. Cisco IOS software decides which primary downstream channel to use for the fiber node from the set of channels assigned with **downstream cable**. Assigning more than one primary channel to a fiber node with the **downstream cable** command can be useful for load-balancing purposes.



### Note

If the primary downstream channel for the fiber node is assigned from a SPA downstream, then the **downstream cable** command is not required.

If a wideband-capable modem registers as a traditional DOCSIS 2.0 modem, it will register on a downstream channel as follows:

- If the modem's fiber node has been assigned a primary downstream channel with the **downstream cable** command, the modem registers on that downstream channel.

If the modem's fiber node has not been assigned a primary downstream channel with the **downstream cable** command, the modem can register on any downstream channel that is visible to it.

For more information on using this command, refer to the *Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide*.

### Examples

The following example shows how to assign a primary downstream channel for fiber node 5. The primary downstream channel is the downstream port located on the cable interface line card at slot/subslot/port 6/0/0.

```
Router# configure terminal
Router(config)# cable fiber-node 5
Router(config-fiber-node)# downstream cable 6/0/0
```

### Related Commands

Command	Description
<b>cable fiber-node</b>	Enters cable fiber-node configuration mode so that you can configure a fiber node.
<b>description (cable fiber-node)</b>	Specifies a description for a fiber node.
<b>downstream modular-cable rf-channel</b>	Specifies the RF channels that are available for wideband channels on a fiber node.
<b>upstream cable connector</b>	Specifies the upstream channel ports for a fiber node.

## downstream integrated-cable rf-channel (interface)

To associate a set of upstream channels to the integrated downstream channels, use the **downstream integrated-cable rf-channel** command in interface configuration mode.

**downstream integrated-cable** *slot/card/port* **rf-channel** *rf-channels* [**upstream grouplist**]

### Syntax Description

<i>slot</i>	Identifies the chassis slot where the Cisco cable interface line card resides. <ul style="list-style-type: none"> <li>• Cisco uBR10012 router—The valid range is from 5 to 8.</li> <li>• Cisco uBR7225VXR router—The valid value is 1 or 2.</li> <li>• Cisco uBR7246VXR router—The valid range is from 3 to 6.</li> </ul>
<i>card</i>	(Cisco uBR10012 only) Secondary slot number of the cable interface line card. The valid subslots are 0 or 1.
<i>port</i>	Downstream port number. <ul style="list-style-type: none"> <li>• Cisco uBR7225VXR router and Cisco uBR7246VXR router—The valid value is 0 or 1.</li> <li>• Cisco uBR10012 router—The valid range is from 0 to 4.</li> </ul>
<b>rf-channel</b> <i>rf-channel</i>	Specifies association of the downstream channels to the channel group descriptor. The valid range is from 0 to 3.
<b>upstream grouplist</b>	Specifies the logical identifier of upstream channels serving these downstream RF channels. The valid range is from 0 to 7.

### Command Default

No default upstream channels are configured with the integrated downstream channels.

### Command Modes

Interface configuration (config-if)

### Command History

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

---

**Examples**

The following example shows how to use the **downstream integrated-cable rf-channel** command on the Cisco uBR10012 router.

```
Router# configure terminal
Router(config)# interface cable 7/0/0
Router(config-if)# downstream integrated-cable 7/0/0 rf-channel 1 upstream 1
```

---

**Associated Features**

The **downstream integrated-cable rf-channel** command is used to configure the following:

- [Configuring the Cisco UBR-MC20X20V Cable Interface Line Card](#)
- [Configuring the Cisco uBR-MC88V Cable Interface Line Card](#)

---

**Related Commands**

Command	Description
<b>cable upstream max-ports</b>	Configures the maximum number of upstreams on a MAC domain on a line card.

# downstream local upstream

To restrict the set of Cisco uBR10-MC5X20 upstreams associated with the Cisco uBR10-MC5X20 downstreams, use the **downstream local upstream** command in interface configuration mode.

**downstream local upstream** *group**list*

## Syntax Description

<i>group</i> <i>list</i>	Specifies the number of upstreams associated with the Cisco uBR10-MC5X20 downstream channels.
--------------------------	-----------------------------------------------------------------------------------------------

## Command Default

All upstreams under the cable interface are associated with the Cisco uBR10-MC5X20 downstreams.

## Command Modes

Interface configuration mode (config-if)

## Command History

Release	Modification
12.3(23)BC	This command was introduced for the Cisco uBR10012 router.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

## Usage Guidelines

Use this command to restrict a set of Cisco uBR10-MC5X20 upstreams to Cisco uBR10-MC5X20 downstreams. This restricts MAC management messages (MMM) to be sent to the specified upstreams only.

## Examples

The following example shows how the **downstream local upstream** command is used in the Cisco uBR10012 router.

```
Router# configure terminal
Router (config)# interface cable 5/1/0
Router(config-if)# downstream local upstream 0-1
```

## Related Commands

Command	Description
<b>downstream cable</b>	Assigns a primary downstream channel for a fiber node.



# downstream modular-cable rf-channel (interface)

To associate a set of Cisco uBR10-MC5X20 upstreams with individual modular downstream channels from the SPA into a given cable MAC domain, use the **downstream modular-cable rf-channel** command in interface configuration mode.

## Cisco IOS Release 12.3(23)BC

**downstream modular-cable** *slot/subslot/bay* **rf-channel** *rf channels* [**upstream grouplist**]

## Cisco IOS Release 12.2(33)SCB and later

**downstream modular-cable** *slot/bay/port* **rf-channel** *rf channels* [**upstream grouplist**]

## Cisco IOS Release 12.2(33)SCE and later

**downstream modular-cable** *slot/subslot/controller* **rf-channel** *rf channels* [**upstream grouplist**]

Syntax Description	
<i>slot</i>	Slot where a SIP resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for SIPs.  For the Cisco uBR-MC3GX60V cable interface line card, the cable interface slot values range from 5 to 8.
<i>subslot</i>	Subslot where a SIP resides. On the Cisco uBR10012 router, subslot 0 is always specified.
<i>bay</i>	Bay in a SIP where a SPA is located. The valid values are 0 (upper bay) and 1 (lower bay).
<i>port</i>	Interface number on the SPA.
<i>controller</i>	Modular-Cable controller number. The valid values are 0 to 2.  <b>Note</b> This option is available only on the Cisco uBR-MC3GX60V cable interface line card and on the Cisco router running Cisco IOS Release 12.2(33)SCE and later releases.
<b>rf-channel</b>	Specifies the association of a continuous range of RF channels within the SPA downstream.
<i>rf channels</i>	Range of RF channel physical ports on the SPA FPGA.
<b>upstream</b>	Specifies a set of ranges of upstream to allow association of a noncontiguous list of upstreams to one or more SPA downstreams. If the range is not specified, all the upstreams in the MAC domain are associated.
<i>grouplist</i>	Number of upstreams with the modular cable downstream channel.

**Command Default** By default, all upstream channels in an interface are associated with the modular downstream channels in the same interface.

**Command Modes** Interface configuration (config-if)

## ■ downstream modular-cable rf-channel (interface)

Command History	Release	Modification
	12.3(23)BC	This command was introduced for the Cisco uBR10012 router.
	12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB. This command was modified to change the addressing format for the modular cable interface from <i>slot/subslot/bay</i> to <i>slot/bay/port</i> .
	12.2(33)SCE	This command was modified to change the valid range of <i>slot</i> .

**Usage Guidelines**

Use this command to create primary-capable channels by associating a single or a set of Cisco uBR10-MC 5X20 upstream channels with individual modular downstream channels on a fiber node. When a primary-capable channel is created, the same modular downstream channel cannot be used as a primary-capable channel in another MAC domain. However, it can be used as non-primary-capable channel in another MAC domain.

**Examples**

The following example shows how to use the **downstream modular-cable rf-channel** command on the Cisco uBR10012 router.

```
Router# configure terminal
Router (config)# interface cable 5/1/0
Router(config-if)# downstream modular-cable 1/0/0 rf-channel 0-2 upstream 0-1 4-5
```

**Related Commands**

Command	Description
<b>downstream modular-cable rf-channel</b>	Specifies the RF channels that are available for wideband channels on a fiber node.
<b>rf-channel cable downstream channel-id</b>	Assigns a downstream channel ID to an RF channel.

# downstream modular-cable rf-channel

To specify the RF channels that are available for wideband channels on a fiber node, use the **downstream modular-cable rf-channel** command in cable fiber-node configuration mode. To remove RF channels that are available for wideband channels on a fiber node, use the **no** form of this command.

## Cisco IOS Release 12.3(23)BC

**downstream modular-cable** *slot/subslot/bay* **rf-channel** {*rf-port* | *low-high*}

**no downstream modular-cable** *slot/subslot/bay* **rf-channel** {*rf-port* | *low-high*}

## Cisco IOS Release 12.2(33)SCB

**downstream modular-cable** *slot/bay/port* **rf-channel** {*rf-port* | *low-high*}

**no downstream modular-cable** *slot/bay/port* **rf-channel** {*rf-port* | *low-high*}

### Syntax Description

<i>slot</i>	The slot where a SIP resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for SIPs.
<i>subslot</i>	The subslot where a SIP resides. On the Cisco uBR10012 router, subslot 0 is always specified.
<i>bay</i>	The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay).
<i>port</i>	Specifies the interface number on the SPA.
<i>rf-port</i>	Specifies the RF channel physical port on the Wideband SPA FPGA. Valid values for <i>rf-port</i> depend on the configuration set with the <b>annex modulation</b> command.
<i>low-high</i>	A range of RF channel physical ports on the Wideband SPA FPGA. The <i>low</i> and <i>high</i> values are separated by a hyphen.

### Command Default

If the **downstream modular-cable rf-channel** command is not issued, no RF channels are configured for wideband channels on the fiber node.

### Command Modes

Cable fiber-node configuration (fiber-node)

### Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SCB	This command was modified to change the addressing format for the modular cable interface from <i>slot/subslot/bay</i> to <i>slot/bay/port</i> .

**Usage Guidelines**

The **downstream modular-cable rf-channel** command makes RF channels available for use on a fiber node. Fiber node software configuration mirrors the physical topology of the cable network. The **cable rf-channel** command configures the RF channels that will be used for a wideband channel on a Wideband SPA.

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

**Note**

Effective with Cisco IOS Release 12.3(23)BC, the **annex modulation** command is obsolete and **annex** and **modulation** are included as keyword options in the **rf-channel frequency** command.

- For annex A and 256 QAM, each Wideband SPA supports 18 RF channels. In this case, valid values for the *rf-port* argument are 0 to 17.
- For all other cases, the SPA supports 24 RF channels. In these cases, valid values for the *rf-port* argument are 0 to 23.

A fiber node can be configured to have RF channels from one or both Wideband SPAs. However, a wideband channel cannot be comprised of RF channels from two different SPAs.

Each time the **downstream modular-cable rf-channel** command is issued for a fiber node, the set of RF channels that are available for use on that fiber node is *added to in a cumulative manner*. For example, if the following **downstream modular-cable rf-channel** commands were issued, the set of RF channels available for fiber node 1 is RF channels 0 to 10 on the Wideband SPA in slot/subslot/bay 1/0/0.

```
Router# configure terminal
Router(config)# cable fiber-node 1
Router(config-fiber-node)# downstream modular-cable 1/0/0 rf-channel 0-5
Router(config-fiber-node)# downstream modular-cable 1/0/0 rf-channel 6-10
```

**Examples**

The following example shows how to specify that RF channels 0 to 7 on a Wideband SPA will be available for use on fiber node 5. The Wideband SPA is located in slot/subslot/bay 1/0/0.

```
Router# configure terminal
Router(config)# cable fiber-node 5
Router(config-fiber-node)# downstream modular-cable 1/0/0 rf-channel 0-7
```

**Related Commands**

Command	Description
<b>cable fiber-node</b>	Enters cable fiber-node configuration mode to configure a fiber node.
<b>description (cable fiber-node)</b>	Specifies a description for a fiber node.
<b>downstream cable</b>	Assigns a primary downstream channel for a fiber node.
<b>upstream cable connector</b>	Specifies the upstream channel ports for a fiber node.

# duration

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

**duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes* [**penalty** *minutes*] {**upstream** | **downstream**} [**enforce**]

**no duration**

Syntax Description		
<i>minutes</i>		Specifies the size of the sliding window (in minutes) during which subscriber usage is monitored. The valid range is 10 to 44640 with a default of 360 (6 hours).
<b>avg-rate</b> <i>rate</i>		Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 kilobits with no default.
<b>sample-interval</b> <i>minutes</i>		Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30, with a default value of 15.
<b>penalty</b> <i>minutes</i>		(Optional) Specifies the period (in minutes) during which a cable modem (CM) can be under penalty. The valid range is 1 to 10080.
<b>upstream</b>		Specifies monitoring of traffic in the upstream direction.
<b>downstream</b>		Specifies monitoring of traffic in the downstream direction.
<b>enforce</b>		(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.

**Command Default** The **duration** value defaults to 360 minutes (6 hours), and the **sample-interval** value defaults to 15 minutes.

**Command Modes** Enforce-rule configuration (enforce-rule)

Command History	Release	Modification
	12.3(9a)BC	This command was introduced. This command replaces the <b>monitoring-duration</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.
	12.2(33)SCD2	The <b>penalty</b> keyword option was added.

## Usage Guidelines



### Note

This command is applicable only after the **monitoring-basics** command is configured with the keyword **legacy**.

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

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



### Note

Changing the **duration** *minutes*, **avg-rate** *rate*, or **sample-interval** *minutes* values resets the byte counters for that particular enforce-rule and begins a new sliding window period.

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

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

When you use the **show running-configuration** command to display the configuration, the keyword options for the **duration** command are truncated. In the following example, “pen” represents **penalty**, “do” represents **downstream**, and “enf” represents **enforce**:

```
Router# show running-configuration
.
.
.
duration 10 avg-rate 1 sample-interval 10 pen 11 do enf
```

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

## Examples

The following example shows an enforce-rule being configured for a sliding window that is 20 minutes in length, an **avg-rate** of 1 kilobit per second, and a sampling interval of every 10 minutes.

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# duration 20 avg-rate 1 sample-interval 10 penalty 11 do enf
```

## Related Commands

Command	Description
<b>cable qos enforce-rule</b>	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
<b>enabled (enforce-rule)</b>	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.

Command	Description
<b>debug cable subscriber-monitoring</b>	Displays enforce-rule debug messages for subscriber traffic management on the Cisco CMTS routers.
<b>monitoring-basics</b>	Specifies the type of monitoring for subscriber traffic management on a Cisco CMTS router.
<b>peak-time1</b>	Specifies peak and offpeak monitoring times on a Cisco CMTS router.
<b>penalty-period</b>	Specifies the period for which an enforced quality of service (QoS) profile should be in force for subscribers who violate their registered QoS profile.
<b>qos-profile registered</b>	Specifies the registered QoS profile that should be used for this enforce-rule. This command is applicable only for DOCSIS 1.0 cable modems.
<b>qos-profile enforced</b>	Specifies a QoS profile that should be enforced when users violate their registered QoS profile. This command is applicable only for DOCSIS 1.0 cable modems.
<b>service-class (enforce-rule)</b>	Specifies a service class (enforced or registered) that should be used for cable modem monitoring in an enforce-rule. This command is applicable for DOCSIS 1.1 or later cable modems.
<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.
<b>weekend duration</b>	Configures different subscriber monitoring options over weekends on a Cisco CMTS router.

# enabled (enforce-rule)

To activate an enforce-rule and begin subscriber traffic management on a Cisco CMTS router, use the **enabled** command in enforce-rule configuration mode. To disable the enforce-rule without deleting it, use the **no** form of this command.

**enabled**

**no enabled**

**Syntax Description** This commands has no keywords or arguments.

**Command Default** Enforce-rules are disabled.

**Command Modes** Enforce-rule configuration (enforce-rule)

## Command History

Release	Modification
12.2(15)BC1	This command was introduced.
12.3(9a)BC	This command was integrated into Cisco IOS Release 12.3(9a)BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

## Usage Guidelines

An enforce-rule is created and configured using the **cable qos enforce-rule** command, but it is not activated until you run the **enabled** command. Use the **no enabled** command to disable an enforce-rule without removing it from the CMTS configuration. When you disable an enforce-rule, all cable modems with that rule's registered QoS profile are no longer tracked by the Subscriber Traffic Management feature and all cable modems in penalty are moved to their registered QoS profile.

## Examples

The following example shows an enforce-rule being enabled:

```
Router# configure terminal
Router(config)# cable qos enforce-rule residential
Router(enforce-rule)# enabled
```

The following example shows an enforce-rule being disabled. The rule remains in the CMTS configuration file.

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

## Related Commands



Command	Description
<b>cable qos enforce-rule</b>	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
<b>qos-profile enforced</b>	Specifies a QoS profile that should be enforced when users violate their registered QoS profiles.
<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 registered</b>	Specifies the registered QoS profile that should be use 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.

# enforced qos-profile

**Note**

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

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

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

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

**Syntax Description**

<i>profile-id</i>	Specifies the QoS profile to be enforced. The valid range is 0 to 16383, with a default of 0.
<b>no-persistence</b>	(Optional) Specifies that the enforced QoS profile should not remain in force when a cable modem reboots. Instead, when a cable modem (CM) that is in the penalty period reboots, it is automatically removed from the penalty period and assigned the QoS profile that is specified in its DOCSIS configuration file.  The default is without this option, so that enforced QoS profiles remain in effect for cable modems across reboots.

**Command Default**

The profile ID defaults to 0, and enforced QoS profiles are persistent across cable modem reboots.

**Command Modes**

Enforce-rule configuration (enforce-rule)

**Command History**

Release	Modification
12.2(15)BC1	This command was introduced.
12.3(9a)BC	This command was replaced by the <b>qos-profile enforced</b> command.

**Usage Guidelines**

Both the originally provisioned QoS profile and the enforced QoS profile must be created on the Cisco CMTS router. This command does not support profiles that are created by the cable modem.

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

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

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

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

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

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



#### Note

In software releases prior to Cisco IOS Release 12.3(9a)BC, the system automatically applies the enforced QoS profile to violators only if the **enforce** keyword has been used with the **activate-rule at-byte-count** command.

## Examples

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

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

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

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

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

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

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

## 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 on a Cisco CMTS router.
<b>cable qos enforce-rule</b>	Creates an enforce-rule to enforce a particular QoS profile for subscriber traffic management and enters enforce-rule configuration mode.
<b>enabled (enforce-rule)</b>	Activates an enforce-rule and begins subscriber traffic management on a Cisco CMTS router.

Command	Description
<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 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.

# exception pxf

To control the core dumps that are generated when an exception occurs in one of the Parallel eXpress Forwarding (PXF) columns, use the **exception pxf** command in global configuration mode. To disable the creation of core dumps during PXF exceptions, use the **no** form of this command.

**exception pxf** { **core-file** *filename* | **flash** *device* | **style** { **full** | **localized** | **minimal** | **smart** } }

**no exception pxf** { **core-file** | **flash** | **style** }

## Syntax Description

<b>core-file</b> <i>filename</i>	Sets the filename for the core-dump file generated during a PXF exception.
<b>flash</b> <i>device</i>	Specifies the Flash memory device on which to save the core-dump file generated during a PXF exception.
<b>style</b>	Specifies the type of core-dump file to be generated during a PXF exception.
<b>full</b>	Creates a full core-dump file of all PXF columns.
<b>localized</b>	Creates a core-dump file of the PXF column that failed, along with its neighboring columns.
<b>minimal</b>	Creates a minimal core-dump file of the PXF exception.
<b>smart</b>	Creates a core-dump file that contains the data related to the PXF exception.

## Defaults

Core dumps are not generated during PXF exceptions.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines



### Caution

Use the **exception pxf** command only under the direction of a technical support representative. Creating a core dump can disrupt network operations. The core dump is a large binary file that can be interpreted only by technical personnel who have access to source code and detailed memory maps.

## Examples

The following example shows how to specify that the Cisco uBR10012 router should create a minimal core-dump file for PXF exceptions, and that this file should be named ubr10k-pxf and be written to the disk1 device:

```
Router# configure terminal
Router(config)# exception pxf style minimal
Router(config)# exception pxf core-file ubr10k-pxf
```

**exception pxf**

```
Router(config)# exception pxf flash disk1:  
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show pxf xcm</a>	Displays the current state of error checking and correcting (ECC) for the External Column Memory (XCM) on the Parallel eXpress Forwarding (PXF) processor.

# facility-alarm (ubr10012)

To set the temperature thresholds at which the Performance Routing Engine (PRE) module generates a critical, major, or minor alarm to warn of potential equipment damage, use the **facility-alarm** command in global configuration mode. To disable the temperature alarms, use the **no** form of this command.

```
facility-alarm {core-temperature | intake-temperature}
               {critical exceed-action shutdown | major [temp] | minor [temp]}
```

```
no facility-alarm {core-temperature | intake-temperature}
                  {critical exceed-action shutdown | major [temp] | minor [temp]}
```

## Syntax Description

<b>core-temperature</b>	Specifies the temperature threshold for the temperature sensors near the center of the PRE module.
<b>intake-temperature</b>	Specifies the temperature threshold for the temperature sensors at the air intake slots.
<b>critical exceed-action shutdown</b>	In Cisco IOS Release 12.2(11)BC1 and later releases, specifies that a critical temperature alarm should shut down the router after two minutes. This was the default behavior in previous releases.
<b>major</b> [temp]	Specifies the temperature, in degrees Centigrade, at which the PRE module generates a major alarm to warn of potential damage from excessive temperatures.  The valid range for <i>temp</i> is 20 to 67 degrees Centigrade, with a default of 58 for the core temperature threshold and 54 for the intake-temperature threshold.
<b>minor</b> [temp]	Specifies the temperature, in degrees Centigrade, at which the PRE module generates a minor alarm to warn of potential damage from excessive temperatures.  The valid range for <i>temp</i> is 20 to 67 degrees Centigrade, with a default of 50 for the core temperature threshold and 45 for the intake-temperature threshold.

## Command Default

If no specific temperature is given, that particular facility alarm is reset to its default value. The default core temperature thresholds are 85 (critical), 58 (major), and 50 (minor). The default intake-temperature thresholds are 72 (critical), 54 (major), and 45 (minor) degrees Centigrade.

In Cisco IOS releases previous to Cisco IOS Release 12.2(11)BC1, a critical alarm automatically shuts down the router after two minutes to prevent temperature damage. In Cisco IOS Release 12.2(11)BC1 and later, a critical alarm by default does not shut down the router.



### Note

The default temperature thresholds for the critical core and intake temperatures were changed in Cisco IOS Release 12.2(11)BC1.

## Command Modes

Global configuration (config)

**Command History**

Release	Modification
12.2(1)XF1	This command was introduced for the Cisco uBR10012 router.
12.2(11)BC1	The <b>critical exceed-action shutdown</b> option was added. In addition, the default value for the core critical temperature threshold was raised from 57 to 67 degrees Centigrade, and the default value for the intake critical temperature threshold was raised from 60 to 85 degrees Centigrade.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

**Usage Guidelines****Note**

The **facility-alarm core-temperature critical** and **facility-alarm intake-temperature critical** commands are available only if the **service internal** command is defined in the configuration.

The PRE module on the Cisco uBR10012 router contains temperature sensors that monitor the temperature at the air intake slots and on the PRE module itself. The **facility-alarm** command configures the router for the temperature thresholds that will generate a minor, major, or critical alarm, so as to notify the system operators of the temperature problem before excessive heat can damage the router or any of its components.

Before Cisco IOS Release 12.2(11)BC1, a critical alarm would also automatically shut down the router after two minutes. Cisco IOS Release 12.2(11)BC1 made this automatic shutdown a configurable option, so that the system operators can decide whether or not a critical alarm should power down the router.

As a general rule, do not disable the automatic shutdown of the router unless you have a systems operator available to immediately respond to any critical temperature alarms, because this could result in system damage. Typically, the primary reason to disable the automatic shutdown would be if you are replacing the fan tray assembly and want to ensure that the router does not power down if the procedure takes longer than expected.

**Note**

A line card also automatically shuts itself down if the temperature exceeds operational levels. In addition, the AC and DC PEMs also automatically power down if they exceed their operational temperature. However, high temperatures could still cause damage to other components if the problem is not quickly resolved.

**Examples**

The following example shows how to configure the Cisco uBR10012 router so that it generates a minor alarm when the intake temperature exceed 55°C:

```
Router# configure terminal
Router(config)# facility-alarm intake-temperature minor 55
```

The following example shows how to configure the Cisco uBR10012 router to automatically shut down if the high temperature continues for more than two minutes:

```
Router# configure terminal
Router(config)# service internal
Router(config)# facility-alarm core-temperature critical exceed-action shutdown
```



The following example shows how to disable the automatic shutdown feature for both the core and intake temperatures. A critical alarm is still generated when the default critical temperatures are exceeded, but the router does not automatically shut itself down:

```
Router# configure terminal
Router(config)# no facility-alarm core-temperature critical exceed-action shutdown
Router(config)# no facility-alarm intake-temperature critical exceed-action shutdown
```

The following commands disable major and minor alarms for both the core and intake temperature thresholds (but critical alarms are still generated):

```
Router# configure terminal
Router(config)# no facility-alarm core-temperature major
Router(config)# no facility-alarm core-temperature minor
Router(config)# no facility-alarm intake-temperature major
Router(config)# no facility-alarm intake-temperature minor
```

#### Related Commands

Command	Description
<b>clear facility-alarm</b>	Clears some or all of the facility alarms on the Cisco uBR10012 router.
<b>show facility-alarm status</b>	Displays the current temperature thresholds that will trigger a facility alarm.

# hccp authentication

To specify the authentication algorithm on a working or protect cable interface, or both use the **hccp authentication** command in cable interface configuration mode. To disable authentication on a Working CMTS or Protect CMTS, use the **no** form of this command.

**hccp group authentication {md5 | text}**

**no hccp group authentication {md5 | text}**

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<b>md5</b>	Authentication algorithm. In Cisco IOS Release 12.1(3a)EC, MD5 is the only authentication algorithm supported.
<b>text</b>	Unencrypted text specification. Rather than automatically encrypting the authentication key-chain when using the MD5 authentication algorithm, Cisco IOS software simply passes the authentication key-chain as standard, unencrypted text.

## Command Default

The default authentication algorithm is MD5.

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.
12.2(15)BC1	Support was added for the Cisco uBR-MC5X20U/S BPE on the Cisco uBR10012 router.
12.3(17a)BC2	Support was added for the Cisco uBR-MC5X20H BPE on the Cisco uBR10012 router.
12.3(21)BC	This command is obsolete on the Cisco uBR7246VXR router.

## Usage Guidelines

Use this command together with the **hccp authentication key-chain** command to enable and specify the type of N+1 redundancy authentication you will use in your protection scheme.

**Examples**

The following example shows how to specify MD5 as the authentication algorithm for group 1:

```
Router(config-if)# hccp 1 authentication md5
```

**Related Commands**

Command	Description
<b>hccp authentication key-chain</b>	Enables authentication on a given interface and specifies one or more keys that can be used to perform authentication for a specified group.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp authentication key-chain

To enable authentication and define one or more authentication keys to use in a specified group, use the **hccp authentication key-chain** command in cable interface configuration mode. To disable authentication, use the **no** form of this command. The key chains you define must match one or more key chains configured in the Working CMTS or Protect CMTS configuration file.

**hccp group authentication key-chain** *key-chain*

**no hccp group authentication key-chain** [*key-chain*]

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>key-chain</i>	A text string matching a key chain in the Working CMTS or Protect CMTS configuration file. A key chain must have at least one key and can have up to 2,147,483,647 keys.

## Command Default

No default behavior or values

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.
12.2(15)BC1	Support was added for the Cisco uBR-MC5X20U/S BPE on the Cisco uBR10012 router.
12.3(17a)BC2	Support was added for the Cisco uBR-MC5X20H BPE on the Cisco uBR10012 router.
12.3(21)BC	This command is obsolete on the Cisco uBR7246VXR router.

## Usage Guidelines

Use this command in conjunction with the **hccp authentication** command to enable and specify the type of 1+1 redundancy authentication you will use in your protection scheme.

**Note**

You cannot perform authentication on a specified group until you have first defined at least one authentication key chain in global configuration mode.

**Examples**

The following excerpt from a configuration file enables authentication using the MD5 algorithm and defines the authentication key “cisco1” for group 1:

```
!  
key chain cisco1  
  key 1  
    key-string abcdefg  
  key 2  
    key-string 123456789  
!  
...  
!  
interface cable 3/0  
  hccp 1 authentication md5  
  hccp 1 authentication key-chain cisco1  
!
```

**Related Commands**

Command	Description
<b>hccp authentication</b>	Specifies the authentication algorithm for the Working CMTS or Protect CMTS.
<b>hccp authentication key-chain</b>	Enables authentication on a given interface and specifies one or more keys that can be used to perform authentication for a specified group.
<b>key-chain</b>	Defines one or more key chains for authentication between the Working CMTS or Protect CMTS.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp bypass version

To enter bypass version mode for a specific Hot Standby Connection-to-Connection Protocol (HCCP) group, in which the hardware and software version checks are not performed before switching over to a protect interface, use the **hccp bypass version** command in privileged EXEC mode.

**hccp group bypass version**

<b>Syntax Description</b>	<i>group</i>	The group number for the specified interface. The valid range is 1 to 255.
---------------------------	--------------	----------------------------------------------------------------------------

<b>Command Default</b>	Normal HCCP operations ( <b>hccp group check version</b> ), where hardware and software version checks are made between the Working and Protect cable interface line cards.
------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)XF1, 12.2(4)BC1	This command was introduced for the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card with the Cisco RF Switch.
	12.2(8)BC2	Support was added for the Cisco uBR10012 router using the Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards with the Cisco RF Switch.
	12.2(11)BC1	Support was added for the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards with the Cisco RF Switch.
	12.2(15)BC1	Support was added for the Cisco uBR-MC5X20U/S BPE on the Cisco uBR10012 router.
	12.3(17a)BC2	Support was added for the Cisco uBR-MC5X20H BPE on the Cisco uBR10012 router.
	12.3(21)BC	This command is obsolete on the Cisco uBR7246VXR router.

<b>Usage Guidelines</b>	By default, the Cisco CMTS verifies that the Working and Protect cable interfaces are using the same versions of software and hardware, so as to avoid potential incompatibilities during a switchover. The hardware check verifies that the Working and Protect cable interface line cards are compatible. The software check verifies that the two cards are running the same major versions of software. If either of these two conditions is not true, the CMTS by default does not perform the switchover.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

You can override these version checks for a particular HCCP group by using the **hccp bypass version** command. After you give this command, the Cisco CMTS does not check the hardware or software versions of the two cable interfaces before performing a switchover. To return to normal HCCP operations, so that version checks are made for a group, use the **hccp check version** command.

**Note**

Two cable interface line cards are compatible when the Protect card has at least the same number of upstreams or downstreams as the Working card. The exceptions to this are that the Cisco uBR-MC16E card can be protected only by another Cisco uBR-MC16E card. Also, the DOCSIS versions of the Cisco uBR-MC16 card can be protected only by another Cisco uBR-MC16C card. You cannot use the Cisco uBR-MC28C card to protect a Cisco uBR-MC16B/C/S card.

**Examples**

The following example shows how to disable the hardware and software version checks for HCCP group number 20. After giving this command, the Cisco CMTS will switchover from the Working to Protect interface in group 20 without first verifying the cards' compatibility:

```
Router# hccp 20 bypass version
Router#
```

**Related Commands**

Command	Description
<b>hccp check version</b>	Exits bypass version mode, and returns to normal HCCP operation.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

## hccp channel-switch

To configure the Cisco CMTS so that a Cisco RF Switch or Vecima (Wavecom) upconverter becomes a Hot Standby Connection-to-Connection Protocol (HCCP) member in a particular HCCP group, use the **hccp channel-switch** command in cable interface configuration mode. To remove the configuration for the Cisco RF Switch or upconverter, use the **no** form of this command.

**hccp group channel-switch** *member-id* *switch-name* **rfswitch-group** *rfswitch-ip-address*  
*module-bitmap* *position*

**hccp group channel-switch** *member-id* *switch-name* **rfswitch-module** *rfswitch-ip-address*  
*module-number* *position*

**hccp group channel-switch** *member-id* *switch-name* **tty-switch** [**aux** | **console** | **vtty**] *line-number*  
*port*

**hccp group channel-switch** *member-id* *switch-name* {**wavecom-hd** | **wavecom-ma**}  
*prot-ip-address* *protect-module* *work-ip-address* *work-module*

**no hccp group channel-switch** *member-id* *switch-name*

### Syntax Description

<i>group</i>	The group number for the specified interface. The valid range is 1 to 255.
<i>member-id</i>	The member number within the specified group. The valid range is 1 to 255.
<i>switch-name</i>	(Optional) Alpha-numeric string specifies the name of the Cisco RF Switch.
<b>rfswitch-group</b>	Specifies that this is the configuration for a Cisco RF Switch group.
<b>rfswitch-module</b>	Specifies that this is the configuration for a Cisco RF Switch module.
<i>rfswitch-ip-address</i>	Specifies the IP address of the Cisco RF Switch to which the CMTS is connected.
<i>module-bitmap</i>	Specifies the module-bitmap in hexadecimal. The valid range is 0 to FFFFFFFF.  <b>Tip</b> See the TAC-authored <i>N+1 Tips and Configuration</i> document on Cisco.com for more information on the format of the bitmap, and for a worksheet that can be used to calculate the bitmap.
<i>module-number</i>	Specifies the module number on the Cisco RF Switch. The valid range is 1 to 255.  <b>Note</b> This setting must be configured on the Cisco RF Switch as well as the Cisco CMTS.
<i>position</i>	Specifies the position for the Working channel on the Cisco RF Switch. The valid range is 1 to 8.
<b>tty-switch</b>	Specifies the configuration of a Cisco RF Switch that is controlled by its TTY line. You can further specify the type of port being used to control the switch. By default, one of the Cisco RF Switch's serial ports is used, or you can use the <b>aux</b> , <b>console</b> , or <b>vtty</b> lines.  <b>Note</b> Ensure that the switch's DIP switch is set to 00.
<b>aux</b>	(Optional) Specifies that the auxiliary port is being used to control the Cisco RF Switch.



<b>console</b>	(Optional) Specifies that the console port is being used to control the Cisco RF Switch.
<b>vty</b>	(Optional) Specifies that a Virtual Terminal connection (Telnet connection) is being used to control the Cisco RF Switch.
<i>line-number</i>	Specifies the line number on which the Cisco RF Switch is receiving control information for this CMTS. The valid range is 0 to 17 for the default serial port, 0 for the aux port, 0 for the console port, and 0 to 99 for the vty port.
<i>port</i>	Specifies the port number being used on the Cisco RF Switch. The valid range is 1 to 255.
<b>wavecom-hd</b>	Specifies that this is the configuration for a Vecima (Wavecom) HD4040 and QHD4040 upconverter.
<b>wavecom-ma</b>	Specifies that this is the configuration for a Vecima (Wavecom) DUAL4040D, MA4040D, or UC4040D upconverter.
<i>prot-ip-address</i>	Specifies the IP address for the upconverter used for the Protect interface used for this cable interface.
<i>protect-module</i>	Specifies the module number on the upconverter used for the Protect interface to be used for this cable interface. The valid range is 1 to 255.
<i>work-ip-address</i>	Specifies the IP address for the upconverter used for the Working interface used for this cable interface.
<i>work-module</i>	Specifies the module number on the upconverter used for the Working interface to be used for this cable interface. The valid range is 1 to 255.

**Command Default**

The CMTS is not configured to use a Cisco RF Switch by default, and no cable interfaces are configured for N+1 redundancy by default.

**Command Modes**

Interface configuration—cable interface only (config-if)

**Command History**

Release	Modification
12.2(4)XF1, 12.2(4)BC1	This command was introduced for the Cisco uBR10012 router, replacing the <b>hccp ds-switch</b> command for use with the Cisco RF Switch.
12.2(8)BC2	Support was added for the Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards on the Cisco uBR10012 router.
12.2(11)BC1	Support was added for the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.
12.3(21)BC	This command is obsolete on the Cisco uBR7246VXR router.

**Usage Guidelines**

You must configure each Working and Protect cable interface for use with the Cisco RF Switch, typically specifying one **hccp channel-switch** command to configure the Cisco RF Switch information, and another **hccp channel-switch** command to configure the upconverter.

The Protect interface is configured with the same **hccp channel-switch** commands as those that are used on the Working interface. However, typically, the same Protect interface is configured with multiple **hccp channel-switch** commands to protect multiple Working interfaces.

### Examples

The following example shows the cable interface 8/1/0 being configured as member 1 for the Working interface of HCCP group 1. This interface is configured to use the Wavecom HD4040 upconverter with the IP address of 10.97.1.21. The upconverter's module number 2 (B) is used for the Protect interface, and module number 16 (P) is used for the Working interface. The interface uses the Cisco RF Switch at IP address 10.97.1.20, using a module bitmap of AA200000 in switch slot 1.

```
Router# configure terminal
Router(config)# interface cable8/1/0
Router(config-if)# hccp 1 working 1
Router(config-if)# hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
Router(config-if)# hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
```

The following example shows the corresponding configuration for the Protect interface for member 1 of HCCP group 1, which is cable interface 5/1/0 on the same chassis. The **hccp channel-switch** commands are identical to those used for cable interface 8/1/0.

```
Router# configure terminal
Router(config)# interface cable5/1/0
Router(config-if)# hccp 1 protect 1 10.97.1.8
Router(config-if)# hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
Router(config-if)# hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
```

Typically, the same Protect interface is used to protect multiple Working cable interfaces. For example, this same interface could be configured as follows to protect a Working interface that is using module number 14 (N) on the same Wavecom HD4040 upconverter, using slot 2 in the RF Switch.

```
Router# configure terminal
Router(config)# interface cable5/1/0
Router(config-if)# hccp 1 protect 2 10.97.1.8
Router(config-if)# hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14
Router(config-if)# hccp 1 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 AA200000 2
```

### Related Commands

Command	Description
<b>hccp check version</b>	Exits bypass version mode, and returns to normal HCCP operation.
<b>hccp ds-switch</b>	Specifies the downstream upconverter module for a Working CMTS or Protect CMTS (deprecated command).
<b>hccp protect</b>	Allows you to configure a Cisco CMTS to be a Protect CMTS for a specified Working CMTS in a 1+1 redundancy environment.
<b>hccp working</b>	Allows you to designate a Cisco CMTS to be a Working CMTS in a 1+1 redundancy environment.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp check version

To exit bypass version mode and return to normal Hot Standby Connection-to-Connection Protocol (HCCP) operations for a specific HCCP group, use the **hccp check version** command in privileged EXEC mode.

**hccp group check version**

<b>Syntax Description</b>	<i>group</i>	The group number for the specified interface. The valid range is 1 to 255.
---------------------------	--------------	----------------------------------------------------------------------------

<b>Command Default</b>	Normal HCCP operations ( <b>hccp group check version</b> ), where hardware and software version checks are made between the Working and Protect cable interface line cards.
------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)XF1, 12.2(4)BC1	This command was introduced for the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card with the Cisco RF Switch.
	12.2(8)BC2	Support was added for the Cisco uBR10012 router using the Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards with the Cisco RF Switch.
	12.2(11)BC1	Support was added for the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards with the Cisco RF Switch.

<b>Usage Guidelines</b>	By default, the Cisco CMTS verifies that the Working and Protect cable interfaces are using the same versions of software and hardware, so as to avoid potential incompatibilities during a switchover. The hardware check verifies that the Working and Protect cable interface line cards are compatible. The software check verifies that the two cards are running the same major versions of software. If either of these two conditions is not true, the CMTS by default does not perform the switchover.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

You can override these version checks for a particular HCCP group by using the **hccp bypass version** command. After you give this command, the Cisco CMTS does not check the hardware or software versions of the two cable interfaces before performing a switchover. To return to normal HCCP operations, so that version checks are made for a group, use the **hccp check version** command.



## Note

Two cable interface line cards are compatible when the Protect card has at least the same number of upstreams or downstreams as the Working card. The exceptions to this are that the Cisco uBR-MC16E card can be protected only by another Cisco uBR-MC16E card. Also, the DOCSIS versions of the Cisco uBR-MC16 card can be protected only by another Cisco uBR-MC16C card. You cannot use the Cisco uBR-MC28C card to protect a Cisco uBR-MC16B/C/S card.

---

**Examples**

The following example shows how to cancel a previous **hccp bypass version** command for HCCP group 1 and to return to normal HCCP operations:

```
Router# hccp 1 check version
Router#
```

---

**Related Commands**

Command	Description
<b>hccp bypass version</b>	Enters bypass version mode for a specific HCCP group, in which the hardware and software version checks are not performed before switching over to a protect interface.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp ds-switch

To specify the downstream upconverter module for a Working CMTS or Protect CMTS, use the **hccp ds-switch** command in cable interface configuration mode. To negate a downstream upconverter assignment, use the **no** form of this command.

**hccp group ds-switch member make host-ipaddr host-module peer-ipaddr peer-module**

**no hccp group ds-switch member**



## Note

This command has been deprecated in current Cisco IOS releases and has been replaced by the **hccp channel-switch** command.

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>member</i>	The member number within the specified group.
<i>make</i>	The maker of the specified upconverter. Currently, only the Wavecom upconverter is supported ( <b>wavecom</b> ).
<i>host-ipaddr</i>	The IP address of the upconverter module <sup>1</sup> to which the host CMTS is connected.
<i>host-module</i>	The upconverter module number to which the host CMTS is connected. This location is expressed as a simple numeric designation.
<i>peer-ipaddr</i>	The IP address of the upconverter module to which the peer (or remote) CMTS is connected.
<i>peer-module</i>	The upconverter module number <sup>1</sup> to which the peer (or remote) CMTS is connected. This location is expressed as a simple numeric designation.

1. The identification of the upconverter module is important to define when the host or peer CMTS is connected to a channel switch housing multiple modules. For example, the Wavecom MA4040D upconverter chassis offers a maximum of 10 independent frequency agile upconverters.

## Command Default

Upconverter specification and activation is disabled by default and must be specified before switching can take place.

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	This command was deprecated and replaced by the <b>hccp channel-switch</b> command.

**Usage Guidelines**

It is necessary to configure the downstream upconverter module for all Protect CMTS and Working CMTS systems. If you do not specify the downstream upconverter module for all Protect CMTS and Working CMTS systems, you cannot switch between a Protect CMTS and Working CMTS.

**Examples**

The following excerpt from a configuration file specifies module 2 on a Wavecom upconverter at IP address 1.1.11.3 as the host switch module connected to Working CMTS 1 and module 1 on the same Wavecom upconverter (with the same IP address location) as the peer or remote switch module connected to the Protect CMTS:

```
hccp 1 working 1
hccp ds-switch 1 wavecom 1.1.11.3 2 1.1.11.3 1
```

**Related Commands**

Command	Description
<b>hccp channel-switch</b>	(replaces the <b>hccp ds-switch</b> command).
<b>hccp protect</b>	Allows you to configure a Cisco CMTS to be a Protect CMTS for a specified Working CMTS in a 1+1 redundancy environment.
<b>hccp working</b>	Allows you to designate a Cisco CMTS to be a Working CMTS in a 1+1 redundancy environment.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp lockdown

To prevent a Working CMTS from automatically switching to a Protect CMTS in the same group, use the **hccp lockdown** command in privileged EXEC mode.

**Note**

This command is applicable only to Working CMTS in a given group. Issuing this command on a Protect CMTS has no effect.

**hccp group lockdown member**

**Syntax Description**

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>member</i>	The member number within the specified group.

**Command Default**

By default, the **hccp lockdown** command is inactive.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

**Usage Guidelines**

Typically the **hccp lockdown** command is used to disable HCCP switchovers before removing the HCCP configuration on the Working interface. Otherwise, when you remove the HCCP configuration from the Working interface, the Protect interface assumes the Working interface has failed and switches over.

You might also want to prevent a Working CMTS from automatically switching back to a Protect CMTS for testing or additional configuration purposes. For example, you might want to fully test protecting cable interfaces on your Cisco CMTS before returning it to protect status.

**Examples**

The following example shows how to activate the lockdown feature of a Working CMTS in group 1:

```
Router# hccp 1 lockdown
```

Related Commands	Command	Description
	<b>hccp unlockout</b>	Negates the effects of the <b>hccp lockdown</b> EXEC command, making the CMTS available for automatic switchover from a Working CMTS to a Protect CMTS.
	<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
	<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.



# hccp protect

To configure a particular cable interface to protect another cable interface in the same group, use the **hccp protect** command in cable interface configuration mode. To undo a particular host cable interface protection assignment, use the **no** form of this command.

**hccp group protect member ipaddr**

**no hccp group protect member**

## Syntax Description

<i>group</i>	The group number of both the Working and Protect cable interfaces. Valid values are any number from 1 to 255, inclusive.
<i>member</i>	The member number of the specified Working cable interface. Valid values are any number from 1 to 255, inclusive.
<i>ipaddr</i>	An IP address for any working interface (other than protected cable interfaces) installed in the Working CMTS that can transmit and receive redundancy status messages.

## Command Default

No default behavior or values

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

## Usage Guidelines

The protect cable interface must be configured identically to the working cable interface, which typically means the interfaces must be the same card type. However, when the Cisco uBR-MC16S card is used, it can be used with either another Cisco uBR-MC16S card or a Cisco uBR-MC16C card.

[Table 26](#) shows how a switchover affects the enhanced spectrum management features of the Cisco uBR-MC16S card.

**Table 26** *Switchover Operation for a Cisco uBR-MC16C/Cisco uBR-MC16S Configuration*

Working Cable Interface	Protect Cable Interface	Operation After Switchover
Cisco uBR-MC16C	Cisco uBR-MC16S	The protect card (Cisco uBR-MC16S) uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the enhanced spectrum management features of the Cisco uBR-MC16S card, as configured on the protect CMTS.
Cisco uBR-MC16S	Cisco uBR-MC16C	The protect card (Cisco uBR-MC16C) uses the same upstream frequency as the working card. If the upstream becomes unstable, the Cisco uBR-MC16C performs only blind frequency hopping.
Cisco uBR-MC16S	Cisco uBR-MC16S	The protect card initially uses the same upstream frequency as the working card, but after the system stabilizes, the protect card continues using the enhanced spectrum management features of the Cisco uBR-MC16S card.

**Examples**

The following example configures host cable interface 4/0 to protect member 2 of group 2 at IP address 1.1.11.2:

```
Router(config)# interface cable 4/0
Router(config-if)# hccp 2 protect 2 1.1.11.2
```

**Related Commands**

Command	Description
<b>cable downstream rf-power</b>	Sets the RF power output level on a cable interface line card with an integrated upconverter (including the ability to specify an override or delta power value for a Protect interface).
<b>hccp working</b>	Configures a specified cable interface to be a working member of a given group.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp resync

To manually synchronize the Inter-database between the Working and Protect interfaces for a particular member in an Hot Standby Connection-to-Connection Protocol (HCCP) group, use the **hccp resync** command in privileged EXEC mode.

**hccp group resync member**

## Syntax Description

<i>group</i>	The group number for the specified interface. The valid range is 1 to 255.
<i>member</i>	The member ID to be resynchronized. The valid range is 1 to 255.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(4)XF1, 12.2(4)BC1	This command was introduced for the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card with the Cisco RF Switch.
12.2(8)BC2	Support was added for the Cisco uBR10012 router using the Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards with the Cisco RF Switch.
12.2(11)BC1	Support was added for the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards with the Cisco RF Switch.

## Usage Guidelines

The Cisco CMTS automatically synchronizes the Working and Protect interfaces to ensure that when a switchover occurs, the Protect interface will run with a configuration that is identical to that of the Working interface. However, if you are troubleshooting HCCP problems, you can manually resynchronize the databases using the **hccp resync** command before performing any switchover tests.



### Note

When a SYNC event command is occurring, CLI commands might be very slow to respond. In particular, if you enter a **show** command at the same time a SYNC event is occurring, the command might respond produce a blank display, or it might display an error message similar to the following:

```
%No response from slot 6/1. Command aborted
```

If this occurs, wait a minute or so and retry the command.

## Examples

The following example shows how to manually resynchronize the Inter-database between the Working and Protect interfaces for member 4 in HCCP group 13:

```
Router# hccp 13 resync 4
```

Router#

Related Commands	Command	Description
	<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
	<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp revertive

To configure a cable interface on a Protect CMTS that has assumed working capacity to automatically revert back to the Working CMTS, use the **hccp revertive** command in cable interface configuration mode. To disable the ability for the specified cable interface to automatically revert back to protect status, use the **no** form of this command.

**hccp group revertive**

**no hccp group revertive**

<b>Syntax Description</b>	<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
---------------------------	--------------	-----------------------------------------------------------------------------------------------------

<b>Command Default</b>	Enabled
------------------------	---------

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

Command History	Release	Modification
	12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
	12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
	12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
	12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
	12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.
	12.3(21)BC	This command is obsolete on the Cisco uBR7246VXR router.

<b>Usage Guidelines</b>	Using this command in conjunction with the <b>hccp reverttime</b> command gives you the ability to set up your protecting cable interfaces to automatically switch between working and protecting capacity without your intervention. Otherwise, whenever a switchover has occurred, you must manually reactivate the failed Working CMTS and manually return the Protect CMTS to protect status using the <b>hccp switch</b> command.
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## Tip

If you are using the **hccp revertive** command on a cable interface, do not also configure the **hccp track** command. Configuring both commands on the same interface can cause multiple switchovers on the same fault.

### Using hccp track with hccp revertive

As a general rule, if you are using the **hccp track** command on a cable interface, do not also configure the **hccp revertive** command without also configuring **no keepalive** on the cable interface. Configuring both commands on the same interface, along with keepalives, can cause multiple switchovers on the same fault.

If you want to use keepalives along with both the **hccp track** and **hccp revertive** commands, use the **hccp track** command on both the Working and Protect interfaces, so that the Working interfaces on the same card track each other and the Protect interfaces on the same card track each other. [Table 27](#) summarizes the guidelines for using these three commands:

**Table 27** Possible hccp track and hccp revertive Configurations

hccp track (Working I/Fs)	hccp track (Protect I/Fs)	hccp revertive	keepalive Configuration
Yes	No	No	keepalive or no keepalive
Yes	No	Yes	no keepalive
Yes	Yes	Yes	keepalive or no keepalive

### Examples

The following example shows cable interface 4/0 on a Protect CMTS in group 2 being configured to automatically revert to protect status after the Working CMTS peer has returned to active duty:

```
router(config)# interface cable 4/0
router(config-if)# hccp 2 revertive
```

### Related Commands

Command	Description
<b>hccp reverttime</b>	Specifies the time that the Working CMTS waits before automatically switching back to a Working CMTS following system switchover.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp reverttime

To specify the amount of time a Protect interface waits before automatically reverting back to a Working interface following a system switchover, use the **hccp reverttime** command in cable interface configuration mode on the Working CMTS. To set the revert-time back to its default value, use the **no** form of this command.

**hccp group reverttime revert-time**

**no hccp group reverttime**

<b>Syntax Description</b>	<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
	<i>revert-time</i>	The amount of time (in minutes) that a Protect interface waits before automatically switching back to a Working interface following a system switchover. The allowable range is 1 to 65,535 minutes, with a default of 30 minutes.

<b>Defaults</b>	30 minutes
-----------------	------------

<b>Command Modes</b>	Interface configuration (cable interface only, on the Working CMTS)
----------------------	---------------------------------------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
	12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
	12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
	12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
	12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

<b>Usage Guidelines</b>	Use this command to configure the revert-time on the cable interfaces on the Working CMTS so that the Working CMTS will automatically resume normal operations and the Protect CMTS will automatically resume normal protect operations, in case an operator forgets to manually switch the Working CMTS back into operation after fixing the original problem.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The Working CMTS first counts down two minutes of suspend time before starting to count down the revert-time. Any failures that occur within this two-minute suspend time are considered part of the same failure.

This means that the actual time that the Working CMTS will attempt to switch back after a switchover is two minutes plus the revert-time. For example, if the revert-time is set to its default of 30 minutes, the Working CMTS will attempt to switch back into operation 32 minutes after the initial switchover to the Protect CMTS.

After the suspend time has occurred, a failure in the Protect CMTS will cause a switchover to the Working CMTS, regardless of whether the revert-time has expired or not. You can force such a failure in the Protect CMTS, and restore the Working CMTS to operation without waiting for the revert-time, by using the **cable power off** and **cable power on** commands to turn off and turn on the protect interface on the Protect CMTS.

When choosing a revert-time, take into account all possible sources of failures, including third-party equipment. For example, an upconverter failure can trigger a switchover to the Protect CMTS. You should configure the revert-time so that the Working CMTS does not switch back into operation until technicians have had sufficient time to fix the equipment failure.

**Tip**

To disable the revert-time feature, use the **no** version of the **hccp revertive** command on the Protect CMTS.

**Examples**

The following example shows cable interface 3/0 on a Working CMTS in group 2 being configured to wait 15 minutes before automatically reverting back to working status after a system switchover:

```
router(config)# interface cable 3/0
router(config-if)# hccp 2 reverttime 15
```

The following example shows how to give the **no** form of this command, which resets the interface back to its default value of 30 minutes.

```
router(config)# interface cable 5/1/0
router(config-if)# no hccp 2 reverttime
```

**Related Commands**

Command	Description
<b>hccp revertive</b>	Configures a cable interface on a Protect CMTS to automatically revert back to a Working CMTS.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.



# hccp switch

To manually switch a Protect CMTS with its Working CMTS peer (or vice versa), use the **hccp switch** command in privileged EXEC mode.

**hccp group switch member**

<b>Syntax Description</b>	<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
	<i>member</i>	The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
	12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
	12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
	12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
	12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.
	12.2(11)BC3	This command is automatically disabled for approximately 2 to 3 seconds after a PRE module switches over to allow the system to stabilize before performing another switchover.

<b>Usage Guidelines</b>	This command overrides any configuration you may have made on your Protect CMTS and Working CMTS using the <b>hccp revert</b> and <b>hccp reverttime</b> commands. In addition, you can issue the <b>hccp switch</b> command on either a Protect CMTS or a Working CMTS to force it to change places with its peer.
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Examples</b>	The following example shows the host Protect CMTS being configured to assume traffic responsibility for member 2 Working CMTS in group 2:
-----------------	-------------------------------------------------------------------------------------------------------------------------------------------

```
Router# hccp 2 switch 2R
```

Related Commands	Command	Description
	<b>hccp lockdown</b>	Prevents a Working CMTS from automatically switching to a Protect CMTS in the same group.
	<b>hccp unlockout</b>	Negates the effects of the <b>hccp lockdown</b> command, making the CMTS available for automatic switchover from a Working CMTS to a Protect CMTS.
	<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
	<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp timers

To configure HELLO packet interval and hold time for a specified group on a Protect CMTS, use the **hccp timers** command in cable interface configuration mode. To erase the HELLO interval and hold time configuration and to assume the default values for each parameter, use the **no** form of this command.

**hccp group timers** *hello-time hold-time*

**no hccp group timers** [*hello-time hold-time*]



## Note

Issuing the **no** form of this command erases any manual HELLO interval and hold time values and automatically resets them to their default values.

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>hello-time</i>	The HELLO packet interval (in milliseconds) between subsequent HELLO packet transmissions. The acceptable range is 1666 to 5,000 milliseconds, inclusive.
<i>hold-time</i>	The time (in milliseconds) that a Protect CMTS will wait before assuming control of voice traffic for a Working CMTS that has failed to acknowledge a series of HELLO packets. The acceptable range is 5,000 to 25,000 milliseconds, inclusive.

## Command Default

The default HELLO interval is 2,000 milliseconds, and the default hold time is 6,000 milliseconds.

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

**Examples**

The following example shows the HELLO interval and hold time on a Protect CMTS in group 2 being configured to 1,750 and 3,000 milliseconds, respectively:

```
Router(config)# interval c4/0
Router(config-if)# hccp 2 timers 1750 3000
```

**Related Commands**

Command	Description
<b>hccp protect</b>	Configures a particular cable interface to protect another peer cable interface in the same group.
<b>hccp working</b>	Configures a specified cable interface to be a working member of a given group.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp track

To configure a cable interface on a Working CMTS or Protect CMTS to enable automatic switchover based on the interface state, use the **hccp track** command in cable interface configuration mode. To disable the automatic switchover based on interface state, use the **no** form of this command.

**hccp group track** [*interface*]

**no hccp group track** [*interface*]

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>interface</i>	Specifies another cable interface (the default is the current cable interface).

## Command Default

Enabled for the current interface

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

## Usage Guidelines

This command enables automatic switchover of one interface when a tracked interface switches over from “up” to “down.”

Typically, this command is used to allow all interfaces on one card to track one another, so that if one interface goes down and switches over to the Protect, all other interfaces can also switch over, allowing the Protect card to assume full operation for these interfaces. This allows support engineers to troubleshoot the problem on the Working interface, or to remove and replace the Working card, if necessary, without interfering with traffic.

### Using hccp track with hccp revertive

As a general rule, if you are using the **hccp track** command on a cable interface, do not also configure the **hccp revertive** command without also configuring **no keepalive** on the cable interface. Configuring both commands on the same interface, along with keepalives, can cause multiple switchovers on the same fault.

If you want to use keepalives along with both the **hccp track** and **hccp revertive** commands, use the **hccp track** command on both the Working and Protect interfaces, so that the Working interfaces on the same card track each other and the Protect interfaces on the same card track each other. [Table 28](#) summarizes the guidelines for using these three commands:

**Table 28** Possible hccp track and hccp revertive Configurations

hccp track (Working I/Fs)	hccp track (Protect I/Fs)	hccp revertive	keepalive Configuration
Yes	No	No	keepalive or no keepalive
Yes	No	Yes	no keepalive
Yes	Yes	Yes	keepalive or no keepalive

### Examples

The following example shows switchover behavior being enabled on a Cisco CMTS in group 2:

```
Router(config)# interface c3/0
Router(config-if)# hccp 2 track
Router(config-if)# keepalive
Router(config-if)#
```

The following example shows two Cisco uBR-LCP2-MC28C cards being used in a Cisco uBR10012 router, with each downstream being configured for a separate HCCP group. The card in slot 5/1 is being configured as the Working interfaces and the card in slot 6/1 is being configured as the Protect interfaces.

The two downstreams on each card track each other, so if one downstream fails and switches over, the other can do so as well, allowing the Protect card to assume full control of both interfaces. Similarly, when the Working interfaces come back into service, both Protect interfaces switch back at the same time.

```
Router(config)# interface cable c5/1/0
Router(config-if)# hccp 1 working 1
Router(config-if)# hccp 1 track c5/1/1
Router(config-if)# keepalive 3
Router(config-if)# exit
Router(config)# interface cable c5/1/1
Router(config-if)# hccp 2 working 1
Router(config-if)# hccp 2 track c5/1/0
Router(config-if)# keepalive 3
Router(config-if)# exit
Router(config)# interface cable c6/1/0
Router(config-if)# hccp 1 protect 1 ip-address-of-mgmt-lan
Router(config-if)# hccp 1 track c6/1/1
Router(config-if)# keepalive 3
Router(config-if)# exit
Router(config)# interface cable c6/1/1
Router(config-if)# hccp 2 protect 1 ip-address-of-mgmt-lan
Router(config-if)# hccp 2 track c6/1/0
Router(config-if)# keepalive 3
Router(config-if)#
```

Related Commands	Command	Description
	<b>keepalive</b>	A global configuration command that allows you to specify the keepalive message transmission interval on a Working CMTS or Protect CMTS. For more specific information, see the <i>Cisco IOS Interface Command Reference</i> on Cisco.com.
	<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
	<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp unlockout

To reverse the effects of the **hccp lockout** command—that is, to make a Working CMTS available for automatic switchover to Protect CMTS, use the **hccp unlockout** command in privileged EXEC mode.

**hccp group unlockout member**

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>member</i>	The member number within the specified group.

## Command Default

By default, the **hccp unlockout** command is active for all groups and members.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

## Usage Guidelines

This command reverses the effect of the **hccp lockout** command. Once you have reconfigured or tested your Protect CMTS, issuing this command manually reintroduces the CMTS back into your 1+1 redundancy protection scheme.



### Note

This command is applicable only on a Working CMTS in a given group. Issuing this command on a Protect CMTS has no effect.

## Examples

The following example shows the lockout feature of a Working CMTS in group 1 being deactivated:

```
hccp 1 unlockout
```



Related Commands	Command	Description
	<b>hccp lockout</b>	Prevents a Working CMTS from automatically switching to a Protect CMTS in the same group.
	<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
	<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hccp working

To designate a cable interface on a CMTS in the specified group to be a Working CMTS, use the **hccp working** command in cable interface configuration mode. To remove a Working CMTS assignment, use the **no** form of this command.

**hccp group working member**

**no hccp group working member**

## Syntax Description

<i>group</i>	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
<i>member</i>	The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.

## Command Default

No default behavior or values

## Command Modes

Interface configuration (cable interface only)

## Command History

Release	Modification
12.1(3a)EC	This command was introduced for the Cisco uBR7200 series routers.
12.1(7)EC1	Support was added for the Cisco uBR-MC16S cable interface line card.
12.2(4)XF1, 12.2(4)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC28C card.
12.2(8)BC2	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR10012 router and Cisco uBR-LCP-MC16C, Cisco uBR-LCP-MC16E, and Cisco uBR-LCP-MC16S cards.
12.2(11)BC1	Support was added for the N+1 (1:n) RF Switch with the Cisco uBR7246VXR router and Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C cards.

## Usage Guidelines

When N+1 HCCP redundancy is configured, the Protect interface switches over and becomes the active interface when it detects a situation similar to the following:

- The Working interface is removed from the chassis, is powered down, or is reset
- The Working interface crashes
- The Working interface no longer sends out regular keepalive messages
- The Working interface loses connectivity with the cable network

The Protect cable interface must be configured identically to the Working cable interface, which typically means the interfaces should be the same card type. However, when the Cisco uBR-MC16S is used, it can be used with either another Cisco uBR-MC16S card or a Cisco uBR-MC16C card.

Table 26 shows how a switchover affects the enhanced spectrum management features of the Cisco uBR-MC16S card.

**Table 0-29 Switchover Operation for a Cisco uBR-MC16C/Cisco uBR-MC16S Configuration**

Working Cable Interface	Protect Cable Interface	Operation After Switchover
Cisco uBR-MC16C	Cisco uBR-MC16S	The protect card (Cisco uBR-MC16S) uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the enhanced spectrum management features of the Cisco uBR-MC16S card, as configured on the protect CMTS.
Cisco uBR-MC16S	Cisco uBR-MC16C	The protect card (Cisco uBR-MC16C) uses the same upstream frequency as the working card. If the upstream becomes unstable, the Cisco uBR-MC16C performs only blind frequency hopping.
Cisco uBR-MC16S	Cisco uBR-MC16S	The protect card initially uses the same upstream frequency as the working card, but after the system stabilizes, the protect card continues using the enhanced spectrum management features of the Cisco uBR-MC16S card.

### Examples

The following example shows cable interface 4/0 being designated as a Working CMTS interface as member number 2 of group 2:

```
Router(config)# interface cable 4/0
Router(config-if)# hccp 2 working 2
```

### Related Commands

Command	Description
<b>hccp protect</b>	Configures a particular cable interface to protect another cable interface in the same group.
<b>show hccp</b>	Displays information for all cable interfaces on which one or more HCCP groups and authentication modes have been configured.
<b>show hccp interface</b>	Displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

# hold-queue

To limit the size of the IP output queue on an interface, use the **hold-queue** command in interface configuration mode. To restore the default values, use the **no** form of this command.

**hold-queue** *length* {**in** | **out**}

**no hold-queue** {**in** | **out**}

## Syntax Description

<i>length</i>	Integer that specifies the maximum number of packets in the queue. The range of valid values is from 0 to 65535.
<b>in</b>	Specifies the input queue. The default is 75 packets. For asynchronous interfaces, the default is 10 packets.
<b>out</b>	Specifies the output queue. The default is 40 packets. For asynchronous interfaces, the default is 10 packets.

## Defaults

Input hold-queue limit is 75 packets.  
Output hold-queue limit is 40 packets.  
Asynchronous interfaces default is 10 packets.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
10.0	This command was introduced.
11.1	The <b>no hold-queue</b> command was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

## Usage Guidelines

### Defaults

The default limits of this command prevent a malfunctioning interface from consuming an excessive amount of memory. There is no fixed upper limit to a queue size.

### Back-to-Back Routing Updates

The default of 10 packets allows the Cisco IOS software to queue a number of back-to-back routing updates. This is the default for asynchronous interfaces only; other media types have different defaults.

### Hold Queues and Priority Queueing

- The hold queue stores packets received from the network that are waiting to be sent to the client. Cisco recommends that the queue size not exceed 10 packets on asynchronous interfaces. For most other interfaces, queue length should not exceed 100.
- The input hold queue prevents a single interface from flooding the network server with too many input packets. Further input packets are discarded if the interface has too many input packets outstanding in the system.
- If you are using priority output queueing, the length of the four output queues is set using the **priority-list** global configuration command. The **hold-queue** command cannot be used to set an output hold queue length in this situation.
- For slow links, use a small output hold-queue limit to prevent storing packets at a rate that exceeds the transmission capability of the link.
- For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and require the hold queue) but can empty the output hold queue quickly when capacity returns.
- You can display the current hold-queue setting and the number of packets that are discarded because of hold-queue overflows by using the **show interfaces** command in user EXEC mode.



#### Caution

Increasing the hold queue can have detrimental effects on network routing and response times. For protocols that use seq/ack packets to determine round-trip times, do not increase the output queue. Dropping packets instead informs hosts to slow down transmissions to match available bandwidth.

This is generally better than having duplicate copies of the same packet within the network (which can happen with large hold queues).

### Examples

The following example shows how to set a small input queue on a slow serial line:

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 in
```

#### Cisco uBR10012 Universal Broadband Router

The following example shows how to modify the input hold queue on a Gigabit Ethernet SPA:

```
Router# configure terminal
Router(config)# interface GigabitEthernet3/0/0
Router(config-if)# hold-queue 30 in
```

### Related Commands

Command	Description
<b>priority-list</b>	Establishes queueing priorities based on the protocol type.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# hw-module bay reload

To reload the software and restart a SPA, use the **hw-module bay reload** command in privileged EXEC mode.

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

**hw-module bay slot/subslot/bay reload**

## Cisco IOS Release 12.2(33)SCB

**hw-module bay slot/bay/port reload**

<b>Syntax Description</b>	<i>slot</i>	The slot where a SIP resides. On the Cisco uBR10012 router, slots 1 and 3 can be used for SIPs.
	<i>subslot</i>	The subslot where a SIP resides. On the Cisco uBR10012 router, subslot 0 is always specified.
	<i>bay</i>	The bay in a SIP where a SPA is located. Valid values are 0 (upper bay) and 1 (lower bay).
	<i>port</i>	Specifies the interface number on the SPA.

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
	12.2(33)SCB	This command was modified to change the addressing format for a SPA from <i>slot/subslot/bay</i> to <i>slot/bay/port</i> .

<b>Usage Guidelines</b>	The <b>hw-module bay reload</b> command reloads the software and restarts a SPA.
-------------------------	----------------------------------------------------------------------------------

<b>Examples</b>	The following example shows how to reload the software for the Cisco Wideband SPA in slot 1, subslot 0, and bay 1.
	<pre>Router# hw-module bay 1/0/1 reload Router#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>hw-module shutdown</b>	Shuts down a PRE1 module, line card, SIP, or SPA.

## hw-module shutdown (ubr10012)

To shut down a particular Performance Routing Engine (PRE1) module, line card, Wideband SIP or Wideband SPA, use the **hw-module shutdown (ubr10012)** command in global configuration mode. To activate a specific PRE1, line card, Wideband SIP or Wideband SPA, use the **no** form of this command.

```
hw-module {main-cpu | pre {A|B} | sec-cpu | slot slot-number | subslot slot/subslot |
bay slot/subslot/bay} shutdown [unpowered]
```

```
no hw-module {main-cpu | pre {A|B} | sec-cpu | slot slot-number | subslot slot/subslot |
bay slot/subslot/bay} shutdown
```

Syntax Description		
<b>main-cpu</b>		Shuts down the PRE1 module that is currently acting as the active PRE1 module.
<b>pre {A B}</b>		Shuts down the PRE1 module that is physically in either PRE slot A (left slot) or PRE slot B (right slot).
<b>sec-cpu</b>		Shuts down the PRE1 module that is currently acting as the standby PRE1 module.
<b>slot slot-number</b>		Shuts down the line cards that are physically present in the specified <i>slot-number</i> (valid range is 1 to 8).
<b>subslot slot/subslot</b>		Shuts down the line card or SIP that is physically present in the slot with the specified slot and subslot numbers. The following are the valid values: <ul style="list-style-type: none"> <li><i>slot</i> = 1 to 8</li> <li><i>subslot</i> = 0 or 1</li> </ul>
<b>bay slot/subslot/bay</b>		Shuts down the SPA in the location specified by the <i>slot/subslot/bay</i> argument. The following are the valid values: <ul style="list-style-type: none"> <li><i>slot</i> = 1 to 3</li> <li><i>subslot</i> = 0 or 1 (0 is always specified)</li> <li><i>bay</i> = 0 (upper bay) or 1 (lower bay)</li> </ul>
<b>unpowered</b>		Used with the Wideband SPA, shuts down the SPA and its interfaces, and leaves them in an administratively down state without power.

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
	12.3(21)BC	Support was added for the Cisco Wideband SIP and Cisco 1-Gbps Wideband SPA.

**Usage Guidelines**

The **hw-module shutdown (ubr10012)** command shuts down in a controlled manner a particular Performance Routing Engine (PRE1) module, line card, Wideband SIP or Wideband SPA. To activate a specific PRE1, line card, Wideband SIP, or Wideband SPA, use the **no** form of this command.

**Caution**

Shutting down the active PRE1 module will trigger a switchover, so that the standby PRE1 module becomes the active PRE1 module.

**Examples**

The following example shows the standby PRE1 module being shut down:

```
Router(config)# hw-module sec-cpu shutdown
Router(config)#
```

The following example shows the active PRE1 module being shut down (which will trigger a switchover to the standby PRE1 module):

```
Router(config)# hw-module main-cpu shutdown
Router(config)#
```

The following example shows the PRE1 module in PRE1 slot B being shut down:

```
Router(config)# hw-module pre B shutdown
Router(config)#
```

**Note**

The **hw-module pre B shutdown** command shuts down the PRE1 module that is physically present in slot B, regardless of whether the module is the active or standby PRE1 module.

The following example shows how to deactivate and verify deactivation for the Cisco Wideband SPA located in slot 1, subslot 0, bay 0. In the output of the **show hw-module bay oir** command, notice the “admin down” in the Operational Status field.

```
Router# configure terminal
Router(config)# hw-module bay 1/0/0 shutdown unpowered
%SPAWBCMTS-4-SFP_MISSING: Wideband-Cable 1/0/0, 1000BASE-SX SFP missing from port 0
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:1, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:2, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:3, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:4, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:5, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:6, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:7, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:8, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:9, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:10, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:11, changed state to down
...
Router# show hw-module bay 1/0/0 oir
```

Module	Model	Operational Status
bay 1/0/0	SPA-24XDS-SFP	admin down

The following example shows how to activate and verify activation for the Cisco Wideband SPA located in slot 1, subslot 0, bay 0. In the output of the **show hw-module bay oir** command, notice the “ok” in the Operational Status field.

```
Router# configure terminal
Router(config)# no hw-module bay 1/0/0 shutdown
```



```

%SPAWCMTS-4-SFP_OK: Wideband-Cable 1/0/0, 1000BASE-SX SFP inserted in port 0
%SPAWCMTS-4-SFP_LINK_OK: Wideband-Cable 1/0/0, port 0 link changed state to up
%SNMP-5-LINK_UP: LinkUp:Interface Wideband-Cable1/0/0:0 changed state to up
%LINK-3-UPDOWN: Interface Cable1/0/0:0, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:1, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:2, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:3, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:4, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:5, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:6, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:7, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:8, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:9, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:10, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:11, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable1/0/0:0, changed state to up
...
Router# show hw-module bay 1/0/0 oir

```

Module	Model	Operational Status
-----	-----	-----
bay 1/0/0	SPA-24XDS-SFP	ok

#### Related Commands

Command	Description
<b>hw-module reset</b>	Resets a PRE1 module or line card.
<b>hw-module reload</b>	Reloads the software in and restarts a Cisco 1-Gbps Wideband SPA.
<b>redundancy</b> <b>force-failover</b> <b>main-cpu</b>	Forces a manual switchover between the active and standby PRE1 modules.

# hw-module slot pos

To configure a line card slot for Packet over SONET (POS) operation, use the **hw-module slot pos** command in privileged EXEC mode. To remove the configuration for a line card slot, use the **no** form of this command.

**hw-module slot** *slot-number* **pos**

**no hw-module slot** *slot-number* **pos**

## Syntax Description

<i>slot-number</i>	Resets the line cards that are physically present in the specified <i>slot-number</i> (valid range is 1 to 8).
--------------------	----------------------------------------------------------------------------------------------------------------

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(11)BC3	This command was introduced for the Cisco uBR10012 OC-48 Dynamic Packet Transport (DPT) Interface Module for the Cisco uBR10012 router.

## Usage Guidelines

You must first use the **hw-module slot pos** command to preconfigure a line card slot for POS operation of the Cisco uBR10012 OC-48 DPT card before you can configure the card with any further commands. You must also use the **card 1oc48dpt/pos-1** command to configure the card slot for the proper card type.



### Note

If you have previously used the **hw-module slot srp** command to configure line card slots for Spatial Reuse Protocol (SRP) operation, you must first cancel that configuration using the **no hw-module slot srp** command before you can configure the slots for POS operation using the **hw-module slot pos** command.

## Examples

The following example shows the Cisco uBR10012 OC-48 DPT line card in slot 3 being configured for POS operation:

```
Router# hw-module slot 3 pos
Router# card 3/0 1oc48dpt/pos-1
```

The following example shows the Cisco uBR10012 OC-48 DPT line cards in slots 3 and 4 being reconfigured from SRP operation to POS operation:

```
Router# no hw-module slot 3 srp
Router# no hw-module slot 4 srp
Router# hw-module slot 3 pos
Router# card 3/0 1oc48dpt/pos-1
Router# hw-module slot 4 pos
```

```
Router# card 4/0 loc48dpt/pos-1
```

**Related Commands**

Command	Description
<b>hw-module reset</b>	Resets a PRE1 module or line card.
<b>hw-module shutdown (ubr10012)</b>	Shuts down a PRE1 module or line card.
<b>hw-module slot srp</b>	Configures a line card slot for SRP operation.

# hw-module slot srp

To configure a line card slot for Spatial Reuse Protocol (SRP) operation, use the **hw-module slot srp** command in privileged EXEC mode. To remove the configuration for a line card slot, use the **no** form of this command.

**hw-module slot** *slot-number* **srp**

**no hw-module slot** *slot-number* **srp**

## Syntax Description

<i>slot-number</i>	Resets the line cards that are physically present in the specified <i>slot-number</i> (valid range is 1 to 8).
--------------------	----------------------------------------------------------------------------------------------------------------

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(11)BC3	This command was introduced for the Cisco uBR10012 OC-48 Dynamic Packet Transport (DPT) Interface Module for the Cisco uBR10012 router.
12.2(33)SCB	This command is obsolete.

## Usage Guidelines

You must first use the **hw-module slot srp** command to preconfigure a line card slot for SRP operation of a pair of Cisco uBR10012 OC-48 DPT cards before you can configure the cards with any further commands. You must also use the **card 1oc48dpt/pos-1** command to configure each card slot for the proper card type.



### Tip

The Cisco uBR10012 OC-48 DPT line cards support SRP operation only when installed in adjacent odd- and even-numbered slots (such as slots 1 and 2 or 3 and 4). You need to use the **hw-module slot srp** command only for the lower-numbered (odd-numbered) slot to preconfigure both slots of the SRP pair.



### Note

If you have previously used the **hw-module slot pos** command to configure line card slots for Packet over SONET (POS) operation, you must first cancel that configuration using the **no hw-module slot pos** command before you can configure the slots for POS operation using the **hw-module slot srp** command.

## Examples

The following example shows the Cisco uBR10012 OC-48 DPT line cards in slots 1 and 2 being configured for POS operation:

```
Router# hw-module slot 1 srp
Router# card 1/0 1oc48dpt/pos-1
Router# card 2/0 1oc48dpt/pos-1
```

The following example shows the Cisco uBR10012 OC-48 DPT line cards in slots 3 and 4 being reconfigured from POS operation to SRP operation:

```
Router# no hw-module slot 3 pos
Router# no hw-module slot 4 pos
Router# hw-module slot 3 srp
Router# card 3/0 1oc48dpt/pos-1
Router# card 4/0 1oc48dpt/pos-1
```

**Related Commands**

Command	Description
<b>hw-module reset</b>	Resets a PRE1 module or line card.
<b>hw-module shutdown (ubr10012)</b>	Shuts down a PRE1 module or line card.
<b>hw-module slot pos</b>	Configures a line card slot for POS operation.

