

Hot-Standby 1+1 Redundancy

This feature module describes the Hot-Standby 1+1 Redundancy feature. It includes information on the benefits of the new feature, supported platforms, related documents, troubleshooting tips, configuration examples, and a detailed command reference.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 4
- Monitoring and Maintaining Hot-Standby 1+1 Redundancy, page 8
- Configuration Examples, page 9
- Command Reference, page 13
- Debug Commands, page 30

Feature Overview

The Hot-Standby 1+1 Redundancy feature offers you the ability to provide high system availability when you configure a Cisco uBR7200 series universal broadband router to wait in hot-standby mode, protecting another Cisco uBR7200 series universal broadband router in case of system failure. The 1+1 redundancy feature provides three- to five-second automatic system recovery time, thus helping to prevent calls from dropping in the system.



Note

It is not uncommon for voice calls in their setup phase to be dropped when a CMTS system failure occurs, even with 1+1 redundancy configured on the cable network.

In order for 1+1 redundancy to operate between a Protect CMTS and its Working CMTS peer, the configuration files for the two routers must be exactly the same, excluding configuration commands specific to 1+1 redundancy. Sections of this feature module describe the necessary differences in configuration between a Protect CMTS and its Working CMTS peer.

Protection Scenarios

Configuration for 1+1 redundancy takes place at the cable modem card interface level. That is, rather than assigning an entire Cisco uBR7200 series to support another Cisco uBR7200 series, you configure individual interfaces on one Cisco uBR7200 series to protect individual interfaces installed in a different Cisco uBR7200 series.

The protection scenario currently available for Cisco uBR7200 series routers is the 1+1 scenario.

1+1 Protection

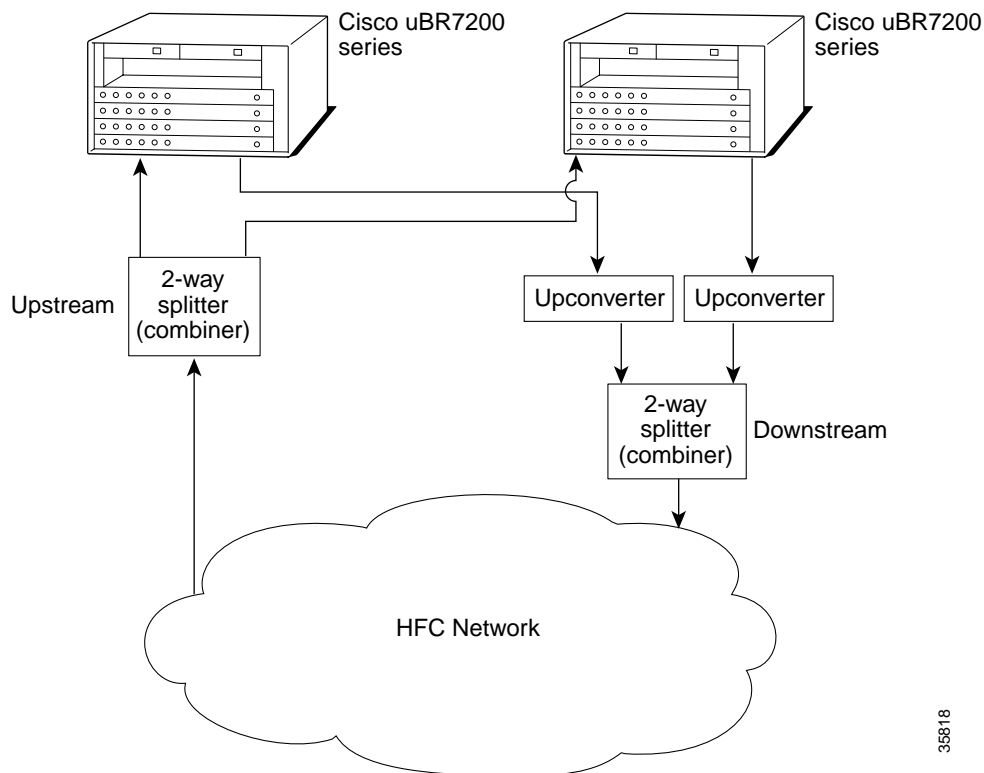
In a 1+1 redundancy protection scheme, the protecting cable modem card interface in the Protect CMTS and working cable modem card interface in the Working CMTS are each connected to the same downstream combiner/splitter and the same upstream combiner/splitter. See Figure 1. In the event of a system failure in the Working CMTS, the Protect CMTS assumes data and voice traffic responsibilities by switching both the upstream and downstream connections at the combiner/splitters from the Working CMTS to the Protect CMTS.



Note

1+1 redundancy protection takes place on an interchassis basis, only. That is, you can't protect cable interfaces on a particular CMTS with cable interfaces installed in the *same* chassis.

Figure 1 Sample Cable Headend Deployment Featuring 1+1 Redundancy Protection



35818

Benefits

High Availability

The 1+1 redundancy feature provides three to five second automatic system recovery time in the event of system failure, thus helping to prevent calls from being dropped unintentionally. System failure in a nonredundancy (unprotected) deployment results in loss of all voice calls in progress as well as all voice calls in setup phase because the CMTS requires human intervention to reconfigure and bring the CMTS back on line.

Related Documents

- *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide*
- *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide*
- *Cisco uBR7200 Series Cable Modem Card Hardware Installation*

Supported Platforms

- Cisco uBR7200 series universal broadband routers

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites


To properly configure and activate 1+1 redundancy, you must be sure that you are running Cisco IOS Release 12.1(3)EC or a later version of IOS on the Cisco uBR7200 series universal broadband routers comprising your 1+1 redundancy CMTS peer system.

Configuration Tasks

See the following sections for configuration tasks for the 1+1 redundancy feature. Each task is either optional or required.

- Configuring a Protect CMTS Cable Interface (Required)
- Configuring a Working CMTS Cable Interface (Required)
- Specifying the Downstream Module Type and Location (Required)
- Configuring 1+1 Redundancy Authentication (Optional)
- Configuring 1+1 Redundancy Timers (Optional)
- Configuring Tracking Capabilities (Optional)
- Configuring Reversion Capabilities (Optional)
- Using the hccp switch EXEC Command (Optional)
- Using the hccp lockout and hccp unlockout EXEC Commands (Optional)

Configuring a Protect CMTS Cable Interface

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 2 protect 2 10.1.2.3	Specifies that cable interface 0 on the cable modem card installed in slot 4 will be assigned to protect member 2 of group 2 and will transmit and receive redundancy status messages using destination IP address 10.1.2.3.
		 <p>Note The IP address you specify when using the hccp protect command can be an IP address for any working interface (other than protected cable interfaces) installed in the Cisco uBR7200 series chassis.</p>
Step 3	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Configuring a Working CMTS Cable Interface

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 1 working 1	Specifies that cable interface 0 on the cable modem card installed in slot 4 will be a working interface designated to be member 1 of group 1.
Step 3	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Specifying the Downstream Module Type and Location

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp ds-switch 1 wavcom 1.1.11.3 2 1.1.11.3 1	Specifies module 2 on a Wavecom upconverter at IP address 1.1.11.3 as the host upconverter 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.
Step 3	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Configuring 1+1 Redundancy Authentication

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 1 authenticate md5	Specifies MD5 as the authentication algorithm for group 1, which will provide automatic key-chain encryption.
Step 3	Router(config-if)# hccp 1 authenticate key-chain cisco1	Enables authentication using the MD5 algorithm and defines the authentication key “cisco1” for group 1.
Step 4	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Configuring 1+1 Redundancy Timers

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 2 timers 750 3000	Configures the HELLO interval and hold time on a Protect CMTS in group 2 to 750 and 3000 milliseconds, respectively.
Step 3	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Configuring Tracking Capabilities

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 2 track	Enables automatic failover behavior based on cable interface state for interfaces in group 2. When the interface state of the cable modem card interface in question moves from “up” to “down,” failover automatically takes place.
Step 3	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Configuring Reversion Capabilities

	Command	Purpose
Step 1	Router(config)# interface cable 4/0	Enters interface configuration mode for cable interface 0 on a cable modem card installed in slot 4 of a Cisco uBR7200 series chassis.
Step 2	Router(config-if)# hccp 2 revert	Enables reversion capability on cable interfaces that are members of group 2.
Step 3	Router(config-if)# hccp 2 reverttime 15	Specifies the time before a Working CMTS that has experienced system failover waits before automatically switching back to a Working CMTS to 15 minutes.
Step 4	Router(config-if)# ^Z Router#	Exits back to EXEC mode so that you can perform verification steps.

Using the hccp switch EXEC Command

Command	Purpose
Router# hccp 2 switch 2	Allows you to manually configure a Protect CMTS or Working CMTS to switchover with its peer.

Using the hccp lockout and hccp unlockout EXEC Commands

Command	Purpose
Router# hccp 2 lockout	Prevents a Working CMTS that is currently sending and receiving data and voice traffic from automatically switching to a Protect CMTS in the same group.
Router# hccp 2 unlockout	Makes a Working CMTS that has been manually placed in lockout state using the hccp lockout command available for automatic or manual switchover to a Protect CMTS.

Verifying Hot-Standby 1+1 Redundancy Configuration

- Step 1 Once a working cable interface has been configured, begin transmitting voice traffic (or a suitable substitute) over the cable interface.
- Step 2 Enter interface configuration mode for the cable interface referred to in Step 1 by entering the **interface cable interface number** command at the privileged EXEC prompt.
- Step 3 Shut down the working cable interface by issuing the **shutdown** command.
- Step 4 Type **^Z** to exit back to privileged EXEC mode.
- Step 5 Enter the **show hccp detail** command at the privileged EXEC prompt to display all 1+1 redundancy information configured on the Cisco uBR7200 series.



Note You can optionally use the **show hccp** or **show hccp brief** commands at this point, however, Cisco recommends that you take advantage of the detailed output that is automatically displayed when you use the **show hccp detail** privileged EXEC command.

```
Router# show hccp detail
```

```
Cable3/0 - Group 2 Working, disabled, blocking
authentication none
hello time 2000 msec, hold time 6000 msec
sync time 1000 msec, suspend time 120000 msec
switch time 240000 msec retries 5
local state is Init
tran 0, out staticsync
last switch reason is none
Member 2 non-functional
  ip addr: working unknown, protect unknown
  downstream wavecom (1.1.11.3/5, 1.1.11.3/6), upstream none
  tran #: SYNC 0, last SYNC_ACK 0, last HELLO_ACK 0
  hold timer expires in never
Cable4/0 - Group 1 Protect, enabled, blocking
authentication md5, key-chain "cisco1"
hello time 2000 msec, hold time 6000 msec
sync time 1000 msec, suspend time 120000 msec
local state is Learn, non-revertive
tran 330, out staticsync
last switch reason is none
hello timer expires in 00:00:01.476
Member 1 standby
  ip addr: working 10.20.111.11, protect 10.20.111.10
  downstream wavecom (1.1.11.3/1, 1.1.11.3/2), upstream none
  tran #: SYNC 0, last SYNC_ACK 16, last HELLO_ACK 330
  hold timer expires in 00:00:05.140
```

Monitoring and Maintaining Hot-Standby 1+1 Redundancy

Use the following new **show** commands to display 1+1 redundancy information on your Protect CMTS and Working CMTS.

Command	Purpose
Router# show hccp	Displays information on any groups associated with cable interfaces.
Router# show hccp interface <i>interface number</i>	Displays information on all groups associated with a specific cable interface.

Configuration Examples

This section provides the following 1+1 redundancy configuration examples:

- Example Router Configuration on Working CMTS
- Example Router Configuration on Protect CMTS

Example Router Configuration on Working CMTS



Note

Arrows to the left of the configuration file indicate command lines specific to Hot-Standby 1+1 Redundancy.

```

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr7246-2
!
boot system tftp /tftpboot/annex4/jzang/ubr7200-p-mz 10.0.0.2
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
ip subnet-zero
no ip domain-lookup
ip host abrick 223.255.254.254
!
!
→ key chain cat
→ key 1
→ key-string abcdefg
→ key 2
→ key-string 123456789
!
interface FastEthernet0/0
ip address 10.20.111.11 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
no keepalive
half-duplex
!
interface Ethernet1/0
ip address 1.1.11.2 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!

```

```

interface Ethernet1/2
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Ethernet1/3
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Cable4/0
  ip address 10.20.111.129 255.255.255.240
  no ip directed-broadcast
  ip helper-address 10.0.0.2
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 441000000
  cable upstream 0 frequency 11408000
  cable upstream 0 power-level 8
  no cable upstream 0 shutdown
  cable upstream 1 shutdown
  cable upstream 2 shutdown
  cable upstream 3 shutdown
  cable upstream 4 shutdown
  cable upstream 5 shutdown
→ hccp 1 working 1
→ hccp 1 ds-switch 1 wavecom 1.1.11.3 2 1.1.11.3 1
→ hccp 1 authentication md5
→ hccp 1 authentication key-chain cat
!
router eigrp 1
  passive-interface Cable4/0
  network 10.20.111.8 0.0.0.7
  network 10.20.111.128 0.0.0.15
!
ip classless
no ip http server
!
snmp-server engineID local 00000009020000D058277000
snmp-server community private RW
snmp-server manager
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  stopbits 1
line vty 0 4
  login
!
end

```

Example Router Configuration on Protect CMTS


Note

Arrows to the left of the configuration file indicate command lines specific to Hot-Standby 1+1 Redundancy.

```

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr7246-1
!
boot system tftp /tftpboot/annex4/jzang/ubr7200-p-mz 10.0.0.2
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
ip subnet-zero
no ip domain-lookup
ip host abrick 223.255.254.254
!
→ key chain cat
→ key 1
→ key-string abcdefg
→ key 2
→ key-string 123456789
!
interface FastEthernet0/0
ip address 10.20.111.10 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
no keepalive
half-duplex
!
interface Ethernet1/0
ip address 1.1.11.1 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown

```

```

!
interface Cable3/0
  no ip address
  no ip directed-broadcast
  ip helper-address 10.0.0.2
  shutdown
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 441000000
  cable upstream 0 frequency 11408000
  cable upstream 0 power-level 10
  no cable upstream 0 shutdown
→ hccp 2 working 2
→ hccp 2 ds-switch 2 wavecom 1.1.11.3 5 1.1.11.3 6
!
interface Cable4/0
  ip address 10.20.111.129 255.255.255.240
  no ip directed-broadcast
  ip helper-address 10.0.0.2
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 441000000
  cable downstream channel-id 0
  cable upstream 0 frequency 11408000
  cable upstream 0 power-level 8
  no cable upstream 0 shutdown
  cable upstream 1 shutdown
  cable upstream 2 shutdown
  cable upstream 3 shutdown
  cable upstream 4 shutdown
  cable upstream 5 shutdown
→ hccp 1 protect 1 10.20.111.11
→ hccp 1 ds-switch 1 wavecom 1.1.11.3 1 1.1.11.3 2
→ hccp 1 authentication md5
→ hccp 1 authentication key-chain cat
!
router eigrp 1
  passive-interface Cable4/0
  network 10.20.111.8 0.0.0.7
  network 10.20.111.128 0.0.0.15
!
ip classless
no ip http server
!
snmp-server engineID local 00000009020000505461E400
snmp-server community private RW
snmp-server manager
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  stopbits 1
line vty 0 4
  login
!
end

```

Command Reference

This section documents new commands related to the 1+1 redundancy feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **hccp authenticate**
- **hccp authenticate key-chain**
- **hccp ds-switch**
- **hccp lockout**
- **hccp protect**
- **hccp revert**
- **hccp reverttime**
- **hccp switch**
- **hccp timers**
- **hccp track**
- **hccp unlockout**
- **hccp working**
- **show hccp**
- **show hccp interface**

hccp authenticate

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

```
hccp group authenticate md5 | text
```

```
no hccp group authenticate { md5 | text }
```

Syntax Description

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

Defaults

The default authentication algorithm is MD5.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Usage Guidelines

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

Examples

The following example specifies MD5 as the authentication algorithm for group 1:

```
interface cable 3/0
  hccp 1 authenticate md5
```

Related Commands

Command	Description
hccp authenticate key-chain	Enables authentication on a given interface and specifies one or more keys that can be used to perform authentication for a specified group.

hccp authenticate key-chain

To enable authentication and define one or more authentication keys to use in a specified group, use the **hccp authenticate key-chain** interface configuration command. 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's configuration file.



Note

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

hccp group authenticate key-chain *key-chain*

no hccp group authenticate 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's configuration file. A key chain must have at least one key and can have up to 2,147,483,647 keys.
Defaults	No default behavior or values.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.1(3)EC	This command was introduced.
Usage Guidelines	Use this command in conjunction with the hccp authenticate command to enable and specify the type of 1+1 redundancy authentication you will use in your protection scheme.	

Examples

The following example 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 authenticate md5
  hccp 1 authenticate key-chain cisco1
!

```

Related Commands

Command	Description
hccp authenticate	Specifies the authentication algorithm for the Working CMTS or Protect CMTS.
key chain	A global configuration command that allows you to define one or more key chains for authentication between Working CMTS or Protect CMTSs. For more specific information, refer to the <i>Cisco IOS Release 12.0 Command Reference Master Index</i> on CCO.

hccp ds-switch

To specify the downstream upconverter module for a Working CMTS or Protect CMTS, use the **hccp ds-switch** interface configuration command. 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
```

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.
<i>host-ipaddr</i>		The IP address of the upconverter module ¹ 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 ¹ 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.

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

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

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

Examples

The following configuration file example 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
hccp protect	Allows you to configure a CMTS to be a Protect CMTS for a specified Working CMTS in a 1+1 redundancy environment.
hccp working	Allows you to designate a CMTS to be a Working CMTS in a 1+1 redundancy environment.

hccp lockdown

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



Note

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

hccp *group* **lockout**

Syntax Description

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

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Usage Guidelines

You might 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 uBR7200 series before returning it to protect status.

Examples

The following example activates the lockout feature of a Working CMTS in group 1:

```
hccp 1 lockdown
```

Related Commands

Command	Description
hccp unlockout	Negates the effects of the hccp lockdown EXEC command, making the CMTS available for automatic switchover from a Working CMTS to a Protect CMTS.

hccp protect

To configure a particular cable interface to protect another cable interface in the same group, use the **hccp protect** interface configuration command. 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	group	The group number of both the Working and Protect cable interfaces. Valid values are any number from 1 to 255, inclusive.
	member	The member number of the specified Working cable interface. Valid values are any number from 1 to 255, inclusive.
	ipaddr	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.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

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

```
interface cable 4/0
  hccp 2 protect 2 1.1.11.2
```

Related Commands	Command	Description
	hccp working	Configures a specified cable interface to be a working member of a given group.

hccp revert

To configure a cable interface on a Protect CMTS that has assumed working capacity to automatically revert back to a Protect CMTS for a specified group, use the **hccp revert** interface configuration command. 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 revert

no hccp group revert

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

Defaults

This command is disabled by default.



Note

This command is disabled by default because some customers may want to perform testing or other such activity on the Protect CMTS's working peer before restoring it to working status.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Usage Guidelines

Using this command in conjunction with the **hccp reverttime** 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 **hccp switch** command.

Examples

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

```
interface cable 4/0
  hccp 2 revert
```

Related Commands

Command	Description
hccp reverttime	Specifies the time the Working CMTS waits before automatically switching back to a Working CMTS following system failover.

hccp reverttime

To specify the amount of time a Working CMTS waits before automatically reverting back to a Working CMTS for a specified group following system failover, use the **hccp reverttime** interface configuration command. To negate a revert-time assignment, use the **no** form of this command.

hccp group reverttime revert-time

no hccp group reverttime

Syntax Description	group	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
	revert-time	The amount of time (in minutes) that a Working CMTS waits before automatically switching back to a Working CMTS following system failover. The allowable range is 1 to 65,535 minutes, inclusive.

Defaults The default time a Working CMTS that has experienced a failover waits before automatically switching back to a Working CMTS is 30 minutes.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

Usage Guidelines Use this command in conjunction with the **hccp revert** command on Working CMTSs to specify your own delay intervals for automatic switchover.

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

```
interface cable 3/0
  hccp 2 reverttime 15
```

Related Commands	Command	Description
	hccp revert	Configures a cable interface on a Protect CMTS in a specified group that has assumed working capacity to automatically revert back to a Protect CMTS.

hccp switch

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

hccp *group* **switch** *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.
Defaults	No default behavior or values.	
Command Modes	EXEC	
Command History	Release	Modification
	12.1(3)EC	This command was introduced.
Usage Guidelines	This command overrides any configuration you may have made on your Protect CMTS and Working CMTSs using the hccp revert and hccp reverttime commands. In addition, you can issue the hccp switch command on either a Protect CMTS or a Working CMTS to force it to change places with its peer.	
Examples	The following example configures the host Protect CMTS to assume traffic responsibility for member 2 Working CMTS in group 2: hccp 2 switch 2	
Related Commands	Command	Description
	hccp lockout	Prevents a Working CMTS from automatically switching to a Protect CMTS in the same group.
	hccp unlockout	Negates the effects of the hccp lockout EXEC command, making the CMTS available for automatic switchover from a Working CMTS to a Protect CMTS.

hccp timers

To configure HELLO packet interval and hold time for a specified group on a Protect CMTS, use the **hccp timers** interface configuration command. To erase your HELLO 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



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 333 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 1,000 to 25,000 milliseconds, inclusive.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Examples

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

```
hccp 2 timers 750 3000
```

Related Commands

Command	Description
hccp protect	Configures a particular cable interface to protect another peer cable interface in the same group.
hccp working	Configures a specified cable interface to be a working member of a given group.

hccp track

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

hccp group track

no hccp group track

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

Defaults	This command is enabled by default.
-----------------	-------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

Usage Guidelines	This command must be used in conjunction with the keepalive IOS command. If no keepalive interval has been configured in the configuration file for the Cisco uBR7200 series, the hccp track command has no affect. Automatic failover occurs if the given interface state moves from “up” to “down.”
-------------------------	---

Examples	The following example enables failover behavior on a CMTS in group 2: <pre>hccp 2 track</pre>
-----------------	--

Related Commands	Command	Description
	keepalive	A global configuration command that allows you to specify the keepalive message transmission interval on Working CMTSs or Protect CMTSs. For more specific information, refer to the <i>Cisco IOS Release 12.0 Command Reference Master Index</i> on CCO.

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** EXEC command.



Note

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

hccp *group* **unlockout**

Syntax Description

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

Defaults

By default, the **hccp unlockout** command is active.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)EC	This command was introduced.

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 reintroduce the CMTS back into your 1+1 redundancy protection scheme.

Examples

The following example deactivates the lockout feature of a Working CMTS in group 1:

```
hccp 1 unlockout
```

Related Commands

Command	Description
hccp lockout	Prevents a Working CMTS from automatically switching to a Protect CMTS in the same group.

hccp working

To designate a cable interface on a CMTS in the specified group to be a Working CMTS, use the **hccp working** interface configuration command. To undo 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.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

Examples The following example designates cable interface 4/0 as member number 2 of group 2 as a Working CMTS interface:

```
interface cable 4/0
  hccp 2 working 2
```

Related Commands	Command	Description
	hccp protect	Configures a particular cable interface to protect another cable interface in the same group.

show hccp

To display information on groups associated with cable interfaces, use the **show hccp** privileged EXEC command.

```
show hccp { group } { brief }
```

Syntax Description

<i>group</i>	A specific group number. Valid values are any number from 1 to 255, inclusive. You can use the optional <i>group</i> variable in the show hccp command to display information for only the specified group.
brief	Gives you the option to display a brief summary of the groups, configuration types, member numbers, and status for cable interfaces.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Examples

The following examples are from the **show hccp** and **show hccp brief** commands:

```
ROUTER# show hccp
Cable4/0 - Group 1 Protect, enabled, blocking
authentication md5, key-chain "cisco1"
hello time 2000 msec, hold time 6000 msec
Member 1 standby
ip addr: working 10.20.111.11, protect 10.20.111.10
downstream wavecom (1.1.11.3/1, 1.1.11.3/2), upstream none
```

```
ROUTER# show hccp brief
Interface Config  Grp Mbr Status
Ca4/0      Protect      1   1  standby
```

Related Commands

Command	Description
show hccp interface	A more directed form of the show hccp command that displays group information for a specific cable interface on which one or more groups and authentication modes have been configured.

show hccp interface

To display information on a group associated with a specific cable interface, use the **show hccp interface** privileged EXEC command.

```
show hccp interface interface { brief }
```

Syntax Description		
	<i>interface</i>	The cable interface for which you want to display group information. The information presented includes groups, configuration types, member numbers, status, authentication algorithms, authentication key chains, timers, IP address assignments, and downstream switch designations for the specified cable interface.
	brief	Gives you the option to display a brief summary of the groups, configuration types, member numbers, and status for a specified cable interface.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)EC	This command was introduced.

Examples The following examples are from the **show hccp interface cable 4/0** and **show hccp interface cable 4/0 brief** commands:

```
ROUTER# show hccp interface cable 4/0
Cable4/0 - Group 1 Protect, enabled, blocking
authentication md5, key-chain "cisco1"
hello time 2000 msec, hold time 6000 msec
Member 1 standby
ip addr: working 10.20.111.11, protect 10.20.111.10
downstream wavecom (1.1.11.3/1, 1.1.11.3/2), upstream none

ROUTER# show hccp interface cable 4/0 brief
Interface Config  Grp Mbr Status
Ca4/0      Protect  1  1  standby
```

Related Commands	Command	Description
	show hccp	A more generalized form of this command that displays group information for all cable interfaces on which one or more groups and authentication modes have been configured.

Debug Commands

This section documents new **debug** commands related to the 1+1 redundancy feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **debug hccp authentication**
- **debug hccp events**
- **debug hccp sync**

debug hccp authentication

To display authentication debug messages for groups, use the **debug hccp authentication** privileged EXEC command. Once you have activated debugging with the **debug hccp events** command, you can use the **debug hccp authentication** command to activate and deactivate additional authentication message output. To disable 1+1 redundancy authentication debug message output, use the **no** form of this command.



Note

The **debug hccp authentication** command is designed to be used in conjunction with, and as an augmentation to, the **debug hccp events** and **debug hccp sync** commands. If neither the **debug hccp events** or **debug hccp sync** command has been activated, activating the **debug hccp authentication** command has no effect on debug message output.

debug hccp authentication

no debug hccp authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Debug message output for 1+1 redundancy authentication is disabled by default.

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Examples

The following example shows the additional 1+1 redundancy authentication debug message output produced when the **debug hccp authentication** command has been activated:

```
Router# debug hccp authentication
```

```
Sep  7 09:51:50.151:HCCP 1 0->1:HELLO Learn tran 31708
Sep  7 09:51:50.151:auth md5 keyid 1 digest B77F65ED 1B38ED5C 87A7037B C006DAFB
```

Related Commands

Command	Description
debug hccp events	Allows you to display all group interaction debug messages.
debug hccp sync	Allows you to display 1+1 redundancy synchronization debug messages.

debug hccp events

To display debug messages for all group interaction, excluding authentication message output, use the **debug hccp events** privileged EXEC command. To disable group debug message output, use the **no** form of this command.



Note

Once you have activated the **debug hccp events** command, you can also activate the **debug hccp authentication** command to provide authentication message output in addition to standard group message output.

debug hccp events

no debug hccp events

Syntax Description

This command has no arguments or keywords.

Defaults

Debug message output for all group interaction is disabled by default.

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Examples

The following example shows group interaction debug message output produced when the **debug hccp events** command has been activated:

```
Router# debug hccp events
```

```
Sep  7 09:51:50.151:HCCP 1 0->1:HELLO Learn tran 31708
```

Related Commands

Command	Description
debug hccp authentication	Allows you to display 1+1 redundancy authentication debug message output once the debug hccp events or debug hccp sync command has been activated.
debug hccp sync	Allows you to display 1+1 redundancy synchronization debug messages.

debug hccp sync

To display 1+1 redundancy synchronization debug messages, use the **debug hccp sync** privileged EXEC command. To disable display 1+1 redundancy synchronization debug message output, use the **no** form of this command.

debug hccp sync

no debug hccp sync

Syntax Description

This command has no arguments or keywords.

Defaults

Debug message output for all group interaction is disabled by default.

Command History

Release	Modification
12.1(3)EC	This command was introduced.

Examples

The following example shows display 1+1 redundancy synchronization debug message output produced when the **debug hccp sync** command has been activated:

```
Router# debug hccp sync

Sep  7 09:57:25.215:HCCP 1 0<-1:SYNC Teach tran 88 type DOCSIS10, tran_sync 82
Sep  7 09:57:25.215:HCCP 1 0->1:SYNC_ACK Learn tran 88
Sep  7 09:57:25.219:DOCSIS10_QOS:qos 1
```

Related Commands

Command	Description
debug hccp authentication	Allows you to display 1+1 redundancy authentication debug message output once the debug hccp events or debug hccp sync command has been activated.
debug hccp events	Allows you to display all group interaction debug messages.

■ debug hccp sync