



Configuring Redundancy

This chapter describes how to configure redundant connections and contains these sections:

- [Configuring Fault Tolerance, page 9-1](#)
- [Configuring HSRP, page 9-5](#)
- [Configuring Interface and Device Tracking, page 9-8](#)
- [Configuring Connection Redundancy, page 9-10](#)
- [Synchronizing the Configuration, page 9-11](#)
- [Configuring a Hitless Upgrade, page 9-13](#)

Configuring Fault Tolerance

This section describes a fault-tolerant configuration. In this configuration, two separate Catalyst 6500 series chassis each contain a CSM-S.



Note

You can also create a fault-tolerant configuration with two CSM-S modules in a single Catalyst 6500 series chassis. You also can create a fault-tolerant configuration in either the secure (router) mode or nonsecure (bridge) mode.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSM-S and the routers on the client side and the servers on the server side. In a redundant configuration, two CSM-S modules perform active and standby roles. Each CSM-S contains the same virtual server, server pool, and real server information. When the **alias** command is configured on the client side and again on the server side, both CSM-S modules can share a client-side IP address and a server-side IP address. From either side, each CSM-S is configured identically, and the network sees the fault-tolerant configuration as a single CSM-S. Only the active CSM-S will respond to ARP requests to the alias IP address. In the case of a failover, the client-side routers and the server-side servers need not change their default gateways, continuing to use the alias IP addresses.

The **alias** command provides functionality similar to HSRP by supplying a floating IP address and a virtual MAC address that servers can use as the default gateway. Although it is possible to create a secure mode fault-tolerant configuration without using the **alias** command, the clients and servers would require reconfiguration in the case of a failover. Client-to-server connections would be lost until after reconfiguration of gateway addresses.

In the nonsecure (bridge) mode, the client-side and server-side VLANs will both have the same IP address. Because the client-side gateway address and static routes will use addresses on the server side (and vice versa) rather than the VLAN address, the **alias** command is not needed.

Configuring fault tolerance requires the following:

- Two CSM-S modules that are installed in the Catalyst 6500 series chassis.
- Identically configured CSM-S modules. One CSM-S is configured as the active; the other is configured as the standby.
- Each CSM-S module connected to the same client-side and server-side VLANs.
- Communication between the CSM-S modules provided by a shared private VLAN.



Note When you configure multiple fault-tolerant CSM-S pairs, do not configure multiple CSM-S pairs to use the same fault-tolerant VLAN. Use a different fault-tolerant VLAN for each fault-tolerant CSM-S pair.



Note If the shared private VLAN should fail, both CSM-S modules would become active, causing connectivity failures.

- A network that sees the redundant CSM-S modules as a single entity.
- Connection redundancy by configuring a link that has a 1-GB per-second capacity. Enable the calendar in the switch Cisco IOS software so that the CSM-S state change gets stamped with the correct time.

The following command enables the calendar:

```
Router# configure terminal
Router(config)# clock timezone WORD offset from UTC
Router(config)# clock calendar-valid
```

Because each CSM-S has a different (non-alias) IP address on the client-side and server-side VLAN, the CSM-S can send health monitor probes (see the [“Configuring Probes for Health Monitoring”](#) section on page 11-1) to the network and receive responses. Both the active and standby CSM-S modules send probes while operational. If the standby CSM-S assumes control, it knows the status of the servers because of the probe responses that it has received.

Connection replication supports both non-TCP connections and TCP connections. Enter the **replicate csrp {sticky | connection}** command in the virtual server mode to configure replication for the CSM-S modules.



Note The default setting for the **replicate** command is disabled.

To use connection replication for connection redundancy, enter these commands:

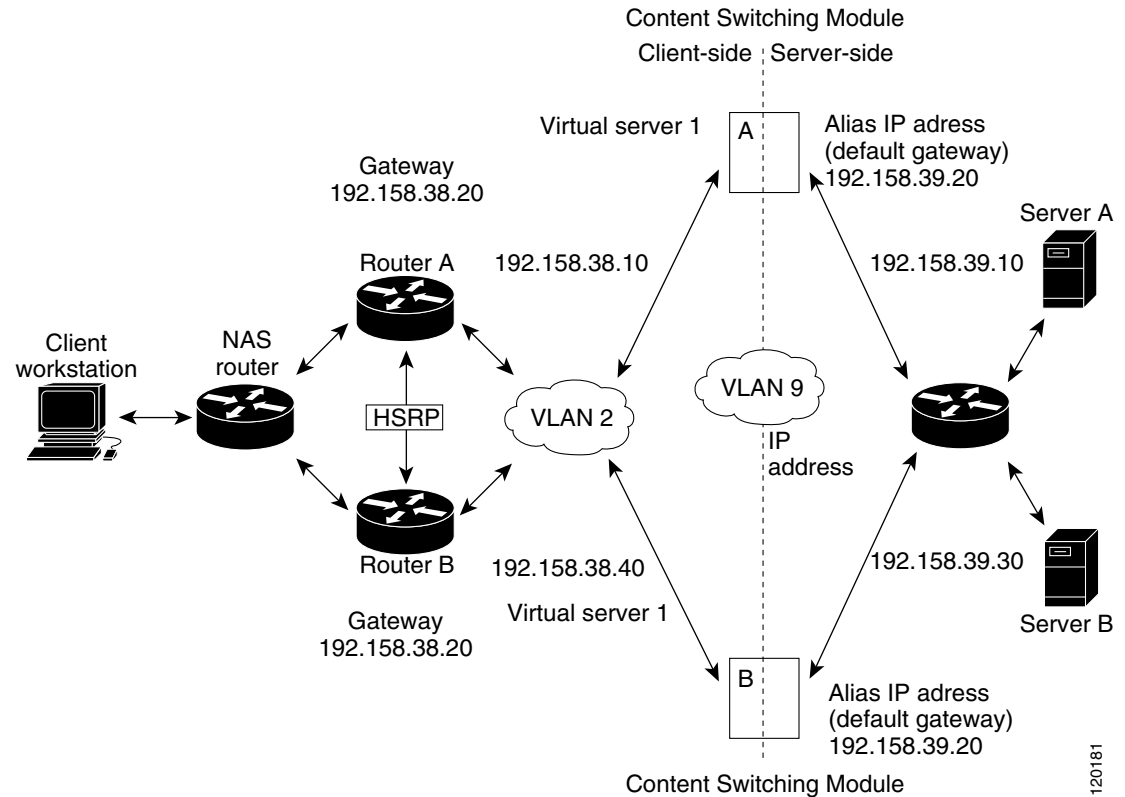
```
Router# configure terminal
Router(config)# no ip igmp snooping
```

The **no ip igmp snooping** command is necessary because the replication frame has a multicast type destination MAC with a unicast IP address. When the switch listens to the Internet Group Management Protocol (IGMP) to find the multicast group membership and build its multicast forwarding information database (FIB), the switch does not find group members and prunes the multicast table. All multicast frames, from active to standby, are dropped causing erratic results.

If no router is present on the server-side VLAN, then each server's default route points to the aliased IP address.

Figure 9-1 shows how the secure (router) mode fault-tolerant configuration is set up.

Figure 9-1 Fault-Tolerant Configuration



Note

The addresses in Figure 9-1 refer to the steps in the following two task tables.

To configure the active (A) CSM-S for fault tolerance, perform this task:

Command	Purpose
Step 1 Router(config-module-csm) # vlan 2 client	Creates the client-side VLAN 2 and enters the SLB VLAN mode ¹ .
Step 2 Router(config-slb-vlan-client) # ip addr 192.158.38.10 255.255.255.0	Assigns the content switching IP address on VLAN 2.
Step 3 Router(config-slb-vlan-client) # gateway 192.158.38.20	(Optional) Defines the client-side VLAN gateway for an HSRP-enabled gateway.
Step 4 Router(config-module-csm) # vserver vip1	Creates a virtual server and enters the SLB vserver mode.

	Command	Purpose
Step 5	Router(config-slb-vserver)# virtual 192.158.38.30 tcp www	Creates a virtual IP address.
Step 6	Router(config-module-csm)# inservice	Enables the server.
Step 7	Router(config-module-csm)# vlan 3 server	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 8	Router(config-slb-vlan-server)# ip addr 192.158.39.10 255.255.255.0	Assigns the CSM-S IP address on VLAN 3.
Step 9	Router(config-slb-vlan-server)# alias ip addr 192.158.39.20 255.255.255.0	Assigns the default route for VLAN 3.
Step 10	Router(config-slb-vlan-server) vlan 9	Defines VLAN 9 as a fault-tolerant VLAN.
Step 11	Router(config-module-csm)# ft group ft-group-number vlan 9	Creates the content switching active and standby (A/B) group VLAN 9.
Step 12	Router(config-module-csm)# vlan	Enters the VLAN mode ¹ .
Step 13	Router(vlan)# vlan 2	Configures a client-side VLAN 2 ² .
Step 14	Router(vlan)# vlan 3	Configures a server-side VLAN 3.
Step 15	Router(vlan)# vlan 9	Configures a fault-tolerant VLAN 9.
Step 16	Router(vlan)# exit	Enters the exit command to have the configuration take effect.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.

To configure the standby (B) CSM-S for fault tolerance, perform this task (see [Figure 9-1](#)):

	Command	Purpose
Step 1	Router(config-module-csm)# vlan 2 client	Creates the client-side VLAN 2 and enters the SLB VLAN mode ¹ .
Step 2	Router(config-slb-vlan-client)# ip addr 192.158.38.40 255.255.255.0	Assigns the content switching IP address on VLAN 2.
Step 3	Router(config-slb-vlan-client)# gateway 192.158.38.20	Defines the client-side VLAN gateway.
Step 4	Router(config-module-csm)# vserver vip1	Creates a virtual server and enters the SLB virtual server mode.
Step 5	Router(config-slb-vserver)# virtual 192.158.38.30 tcp www	Creates a virtual IP address.
Step 6	Router(config-module-csm)# inservice	Enables the server.
Step 7	Router(config-module-csm)# vlan 3 server	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 8	Router(config-slb-vserver)# ip addr 192.158.39.30 255.255.255.0	Assigns the CSM-S IP address on VLAN 3.
Step 9	Router(config-slb-vserver)# alias 192.158.39.20 255.255.255.0	Assigns the default route for VLAN 2.
Step 10	Router(config-module-csm) vlan 9	Defines VLAN 9 as a fault-tolerant VLAN.

	Command	Purpose
Step 11	Router(config-module-csm) # ft group <i>ft-group-number</i> vlan 9	Creates the CSM-S active and standby (A/B) group VLAN 9.
Step 12	Router(config-module-csm) # show module csm all	Displays the state of the fault-tolerant system.

1. Enter the **exit** command to leave a mode or submenu. Enter the **end** command to return to the menu's top level.

Configuring HSRP

This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see [Figure 9-2](#)) and describes how to configure the CSM-S modules with HSRP and CSM-S failover on the Catalyst 6500 series switches.

HSRP Configuration Overview

[Figure 9-2](#) shows that two Catalyst 6500 series switches, Switch 1 and Switch 2, are configured to route from a client-side network (10.100/16) to an internal CSM-S client network (10.6/16, VLAN 136) through an HSRP gateway (10.100.0.1). The configuration shows the following:

- The client-side network is assigned an HSRP group ID of HSRP ID 2.
- The internal CSM-S client network is assigned an HSRP group ID of HSRP ID 1.



Note

HSRP group 1 must have tracking turned on so that it can track the client network ports on HSRP group 2. When HSRP group 1 detects any changes in the active state of those ports, it duplicates those changes so that both the HSRP active (Switch 1) and HSRP standby (Switch 2) switches share the same knowledge of the network.

In the example configuration, two CSM-S modules (one in Switch 1 and one in Switch 2) are configured to forward traffic between a client-side and a server-side VLAN:

- Client VLAN 136



Note

The client VLAN is actually an internal CSM-S VLAN network; the actual client network is on the other side of the switch.

- Server VLAN 272

The actual servers on the server network (10.5/1) point to the CSM-S server network through an alias gateway (10.5.0.1), allowing the servers to run a secure subnet.

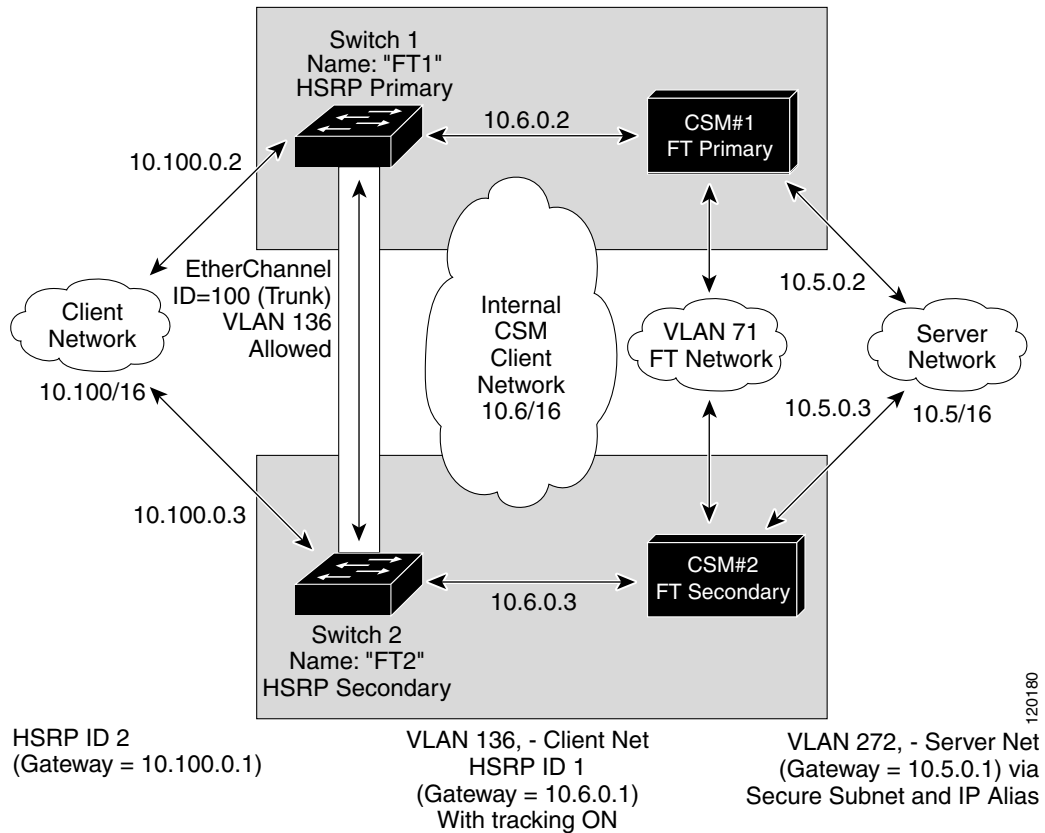
In the example configuration, an EtherChannel is set up with trunking enabled, allowing traffic on the internal CSM-S client network to travel between the two Catalyst 6500 series switches. The setup is shown in [Figure 9-2](#).



Note

EtherChannel protects against a severed link to the active switch and a failure in a non-CSM-S component of the switch. EtherChannel also provides a path between an active CSM-S in one switch and another switch, allowing the CSM-S modules and switches to fail over independently, providing an extra level of fault tolerance.

Figure 9-2 HSRP Configuration



Creating the HSRP Gateway

This section describes how to create an HSRP gateway for the client-side network. The gateway is HSRP ID 2 for the client-side network.



Note

In this example, HSRP is set on Fast Ethernet ports 3/6.

To create an HSRP gateway, perform these steps:

Step 1 Configure Switch 1—FT1 (HSRP active) as follows:

```
Router(config)# interface FastEthernet3/6
Router(config)# ip address 10.100.0.2 255.255.0.0
Router(config)# standby 2 priority 110 preempt
Router(config)# standby 2 ip 10.100.0.1
```

Step 2 Configure Switch 2—FT2 (HSRP standby) as follows:

```
Router(config)# interface FastEthernet3/6
Router(config)# ip address 10.100.0.3 255.255.0.0
Router(config)# standby 2 priority 100 preempt
Router(config)# standby 2 ip 10.100.0.1
```

Creating Fault-Tolerant HSRP Configurations

This section describes how to create a fault-tolerant HSRP secure-mode configuration. To create a nonsecure-mode configuration, enter the commands described with these exceptions:

- Assign the same IP address to both the server-side and the client-side VLANs.
- Do not use the **alias** command to assign a default gateway for the server-side VLAN.

To create fault-tolerant HSRP configurations, perform these steps:

Step 1 Configure VLANs on HSRP FT1 as follows:

```
Router(config)# module csm 5
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.245 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit
```

```
Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.2 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit
Router(config-module-csm)# exit
```

```
Router(config)# vlan 71
Router(config-vlan)# exit
```

```
Router(config)# module csm 5
Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 30
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit
```

```
Router(config-module-csm)# interface vlan136
Router(config-if)# ip address 10.6.0.2 255.255.0.0
Router(config-if)# standby 1 priority 100 preempt
Router(config-if)# standby 1 ip 10.6.0.1
Router(config-if)# standby 1 track Fa3/6 10
```

Step 2 Configure VLANs on HSRP FT2 as follows:

```
Router(config)# module csm 6
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.246 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit
```

```
Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.3 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit
Router(config-module-csm)# exit
```

```

Router(config)# vlan 71
Router(config-vlan)# exit

Router(config)# module csm 6
Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 20
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit

Router(config-module-csm)# interface vlan136
Router(config-if)# ip address 10.6.0.3 255.255.0.0
Router(config-if)# standby 1 priority 100 preempt
Router(config-if)# standby 1 ip 10.6.0.1
Router(config-if)# standby 1 track Fa3/6 10

```



Note To allow tracking to work, preempt must be on.

Step 3 Configure EtherChannel on both switches as follows:

```

Router(console)# interface Port-channel100
Router(console)# switchport
Router(console)# switchport trunk encapsulation dot1q
Router(console)# switchport trunk allowed vlan 136

```



Note By default, all VLANs are allowed on the port channel.

Step 4 To prevent problems, remove the server and fault-tolerant CSM-S VLANs as follows:

```

Router(console)# switchport trunk remove vlan 71
Router(console)# switchport trunk remove vlan 272

```

Step 5 Add ports to the EtherChannel as follows:

```

Router(console)# interface FastEthernet3/25
Router(console)# switchport
Router(console)# channel-group 100 mode on

```

Configuring Interface and Device Tracking

When you configure fault-tolerant HSRP, the active and standby state of the CSM-S does not follow the state of the active HSRP group. When the active HSRP is in one chassis and the active CSM-S is in another chassis, traffic traverses through the trunk ports between the two chassis.

You can configure tracking to track the state of HSRP groups, physical interfaces, and gateways.

Tracking an HSRP Group

You can configure HSRP group tracking so that when the HSRP state changes for a specified tracked group, the Cisco IOS software sends a message to the CSM-S to make an active switchover.

To configure HSRP group tracking, perform this task in the fault-tolerant submode:

Command	Purpose
Router(config-slb-ft)# track group <i>group_number</i>	Specifies the tracked HSRP group.

Tracking a Gateway

When you configure gateway tracking, the Cisco IOS software sends the configured gateway IP address and next hop IP address to the CSM-S. The CSM-S then periodically checks for the availability of the gateway. If the gateway is not available, the CSM-S forces an active switchover.

To configure gateway tracking, perform this task in the fault-tolerant submode:

Command	Purpose
Router(config-slb-ft)# track gateway <i>ip_addr</i>	Specifies the tracked gateway IP address.

Tracking an Interface

You can configure interface tracking so that when the specified physical interface goes down, the Cisco IOS software sends a message to the CSM-S to make an active switchover.

To configure interface tracking, perform this task in the fault-tolerant submode:

Command	Purpose
Router(config-slb-ft)# track interface { async ctunnel dialer fastethernet gigabitethernet }	Specifies the tracked interface.



Note

Although the CLI accepts more arguments than are shown in the **track interface** command description, the CSM supports only physical interfaces for the tracking feature.

Configure the Tracking Mode

To configure the tracking mode, perform this task in the fault-tolerant submode:

Command	Purpose
Router(config-slb-ft)# track mode { any all }	<p>Specifies the tracking mode.</p> <p>The any keyword forces a switchover if any of the tracking devices goes down or if the HSRP state changes to standby.</p> <p>The all keyword forces a switchover when at least one of the tracking devices goes down for every configured tracking feature (group, gateway, and interface).</p>

Configuring Connection Redundancy

Connection redundancy prevents open connections from ceasing to respond when the active CSM-S fails and the standby CSM-S becomes active. With connection redundancy, the active CSM-S replicates forwarding information to the standby CSM-S for each connection that is to remain open when the active CSM-S fails over to the standby CSM-S.

To configure connection redundancy, perform this task:

	Command	Purpose
Step 1	Router# configure terminal	Enters router configuration mode.
Step 2	Router(config)# no ip igmp snooping	Removes IGMP snooping from the configuration.
Step 3	Router(config-module-csm)# vserver <i>virtserver-name</i>	Identifies a virtual server and enters the virtual server submode.
Step 4	Router(config-slb-vserver)# virtual <i>ip-address</i> [<i>ip-mask</i>] <i>protocol</i> <i>port-number</i> [service <i>ftp</i>]	Configures the virtual server attributes.
Step 5	Router(config-slb-vserver)# serverfarm <i>serverfarm-name</i>	Associates a server farm with a virtual server.
Step 6	Router(config-slb-vserver)# sticky <i>duration</i> [group <i>group-id</i>] [netmask <i>ip-netmask</i>]	Ensures that connections from the same client use the same real server.
Step 7	Router(config-slb-vserver)# replicate <i>csrp</i> sticky	Enables sticky replication.
Step 8	Router(config-slb-vserver)# replicate <i>csrp</i> connection	Enables connection replication.
Step 9	Router(config-slb-vserver)# inservice	Enables the virtual server for load balancing.
Step 10	Router(config-module-csm)# ft <i>group</i> <i>group-id</i> vlan <i>vlanid</i>	Configures Router fault tolerance and enters the fault-tolerance submode.

	Command	Purpose
Step 11	Router(config-slb-ft)# priority <i>value</i>	Sets the priority of the CSM-S.
Step 12	Router(config-slb-ft)# failover <i>failover-time</i>	Sets the time for a standby CSM-S to wait before becoming an active CSM-S.
Step 13	Router(config-slb-ft)# preempt	Allows a higher priority CSM-S to take control of a fault-tolerant group when it comes online.

This example shows how to set fault tolerance for connection redundancy:

```
Router(config-module-csm)# vserver VS_LINUX-TELNET
Router(config-slb-vserver)# virtual 10.6.0.100 tcp telnet
Router(config-slb-vserver)# serverfarm SF_NONAT
Router(config-slb-vserver)# sticky 100 group 35
Router(config-slb-vserver)# replicate csrp sticky
Router(config-slb-vserver)# replicate csrp connection
Router(config-slb-vserver)# inservice
Router(config-slb-vserver)# exit
Router(config-module-csm)# ft group 90 vlan 111
Router(config-slb-ft)# priority 10
Router(config-slb-ft)# failover 3
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit
```

Synchronizing the Configuration

You can synchronize the configuration between the active and standby CSM-S in a single chassis or in separate chassis. Synchronization happens over the fault-tolerant VLAN.



Note

Traffic over the fault-tolerant VLAN uses broadcast packets; therefore, we recommend that you remove all devices, other than those necessary for communication between the active and standby CSM-S, from the fault-tolerant VLAN.



Note

It is important that you follow the procedures in this section as described. If you do not enter the **alt standby_ip_address** command on the active CSM-S (as described in [Step 4](#) below) before you synchronize the configuration, the VLAN IP addresses on the standby CSM-S will be removed.

To configure synchronization on the active CSM-S, perform this task:

	Command	Purpose
Step 1	Router# configure terminal	Enters router configuration mode.
Step 2	Router(config)# module <i>csm</i> <i>slot-number</i>	Specifies the slot number of the active CSM-S.
Step 3	Router(config-module-csm)# vlan <i>vlan_ID</i> { <i>client</i> <i>server</i> }	Configures the client-side and server-side VLAN.

	Command	Purpose
Step 4	Router(config-slb-vlan-client)# ip addr <i>active_ip_addr netmask</i> alt <i>standby_ip_addr netmask</i>	Configures an IP address to the CSM-S on this particular VLAN. Enter the alt keyword to specify an alternate IP address that is sent to the standby CSM-S. Note If you do not enter the alt <i>standby_ip_address</i> command on the active CSM-S before you synchronize the configuration, the VLAN IP addresses on the backup CSM-S will be removed
Step 5	Router(config-slb-vlan-client)# exit	Exits VLAN config mode.
Step 6	Router(config-module-csm)# ft group <i>group-id</i> vlan <i>vlanid</i>	Configures fault tolerance and enters the fault-tolerance submode.
Step 7	Router(config-slb-ft)# priority <i>active_value</i> alt <i>standby_value</i>	Sets the priority of the CSM-S. Enter the alt keyword to specify an alternate priority value that is sent to the standby CSM-S.

To configure synchronization on the standby CSM-S, perform this task:

	Command	Purpose
Step 1	Router# configure terminal	Enters router configuration mode.
Step 2	Router(config)# module csm <i>slot-number</i>	Specifies the slot number of the standby CSM-S.
Step 3	Router(config-module-csm)# ft group <i>group-id</i> vlan <i>vlanid</i>	Configures fault tolerance and specifies the fault tolerant VLAN.

To synchronize the configuration, perform this task on the active CSM-S:

	Command	Purpose
	Router# hw-module csm <i>slot-number</i> standby config-sync	Synchronizes the configuration. Enter this command every time you want to synchronize the configuration.

This example shows how to configure both the active and the standby CSM-S for synchronization:

- Active CSM-S:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# module csm 5
Router(config-module-csm)# vlan 130 client
Router(config-slb-vlan-client)# ip addr 123.44.50.5 255.255.255.0 alt 123.44.50.7
255.255.255.0
Router(config-slb-vlan-client)# gateway 123.44.50.1
Router(config-slb-vlan-client)# exit
Router(config-module-csm)# vlan 150 server
Router(config-slb-vlan-server)# ip addr 123.46.50.6 255.255.255.0 alt 123.44.40.8
255.255.255.0
Router(config-slb-vlan-server)# alias 123.60.7.6 255.255.255.0
Router(config-slb-vlan-server)# route 123.50.0.0 255.255.0.0 gateway 123.44.50.1
Router(config-slb-vlan-server)# exit
Router(config-module-csm)# ft group 90 vlan 111
Router(config-slb-ft)# priority 10 alt 15
Router(config-slb-ft)# end
```

- Standby CSM-S:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# module csm 6
Router(config-module-csm)# ft group 90 vlan 111
Router(config-slb-ft)# end
```

This example shows how to synchronize the configuration between the active and standby CSM-Ss:

```
Router# hw-module csm 5 standby config-sync
%CSM_SLB-6-REDUNDANCY_INFO:Module 5 FT info:Active:Bulk sync started
%CSM_SLB-6-REDUNDANCY_INFO:Module 5 FT info:Active:Manual bulk sync completed
```

Configuring a Hitless Upgrade

A hitless upgrade allows you to upgrade to a new software version without major service disruption due to the downtime for the upgrade. To configure a hitless upgrade, perform these steps:

-
- Step 1** If you have preempt enabled, turn it off.
 - Step 2** Perform a write memory on the standby CSM-S.
 - Step 3** Upgrade the standby CSM-S with the new release, and then reboot the CSM-S.
The standby CSM-S boots as standby with the new release. If you have sticky backup enabled, keep the standby CSM-S in standby mode for at least 5 minutes.
 - Step 4** Upgrade the active CSM-S.

Step 5 Reboot the active CSM-S.

When the active CSM-S reboots, the standby CSM-S becomes the new active CSM-S and takes over the service responsibility.

Step 6 The rebooted CSM-S comes up as the standby CSM.
