Configuring Redundant Connections

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

Configuring Fault Tolerance

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

Note You can also create a fault-tolerant configuration with two CSMs 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 and the routers on the client side and the servers on the server side. In a redundant configuration, two CSMs perform active and standby roles. Each CSM contains the same IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM is configured identically. The network sees the fault-tolerant configuration as a single CSM.

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

Configuring fault tolerance requires the following:

- Two CSMs that are installed in the Catalyst 6500 series chassis.
- Identically configured CSMs. One CSM is configured as the active; the other is configured as the standby.
- Each CSM connected to the same client-side and server-side VLANs.
- Communication between the CSMs provided by a shared private VLAN.
- A network that sees the redundant CSMs 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 state change gets stamped with the correct time.

  The following command enables the calendar:

```
Cat6k-2# configure terminal
Cat6k-2(config)# clock timezone WORD offset from UTC
Cat6k-2(config)# clock calendar-valid
```

Because each CSM has a different IP address on the client-side and server-side VLAN, the CSM can send health monitor probes (see the "Configuring Probes for Health Monitoring" section on page 9-1) to the network and receive responses. Both the active and standby CSMs send probes while operational. If the passive CSM assumes control, it knows the status of the servers because of the probe responses 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 CSMs.

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

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

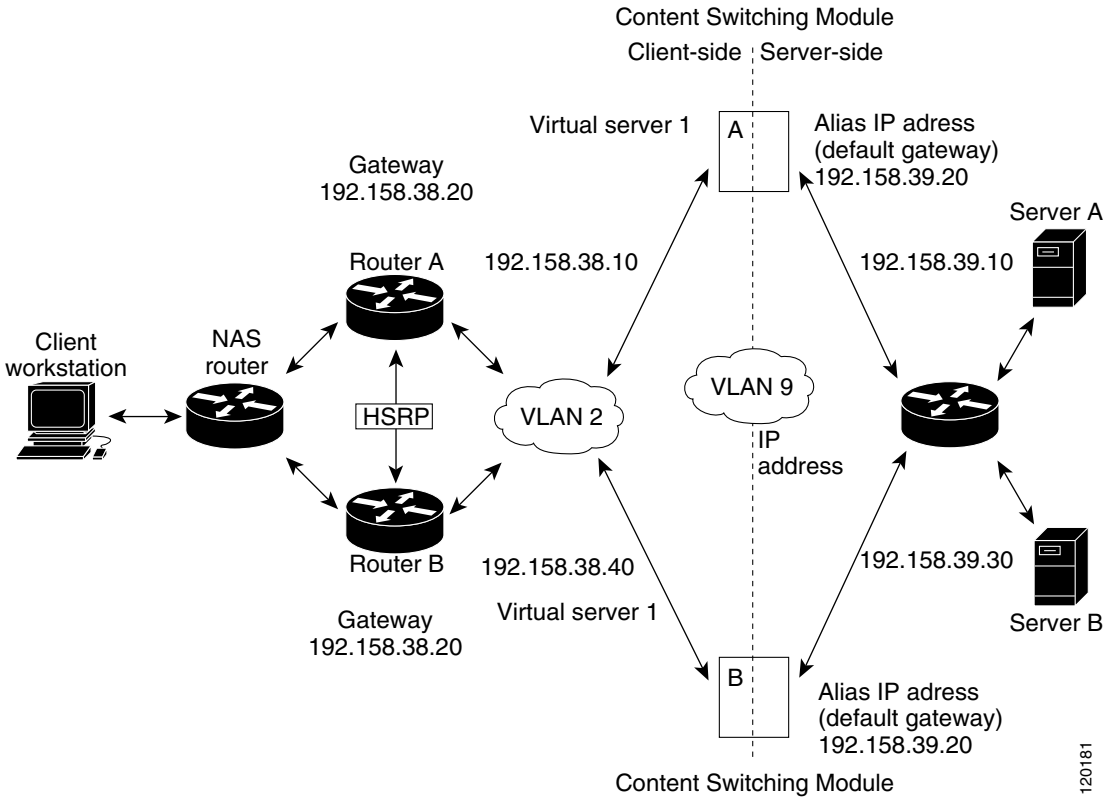
```
Cat6k-2# configure terminal
Cat6k-2(config)# no ip igmp snooping
```

You need to enter the **no ip igmp snooping** command 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 7-1 shows how the secure (router) mode fault-tolerant configuration is set up.

Figure 7-1 Fault-Tolerant Configuration



Note The addresses in Figure 7-1 refer to the steps in the following two task tables.

To configure the active (A) CSM 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 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 affect.

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 for fault tolerance, perform this task (see Figure 7-1):

	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 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` *`ft-group-number`* `vlan 9`	Creates the CSM 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 submode. 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 7-2) and describes how to configure the CSMs with HSRP and CSM failover on the Catalyst 6500 series switches.

HSRP Configuration Overview

Figure 7-2 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 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 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 CSMs (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 VLAN network; the actual client network is on the other side of the switch.

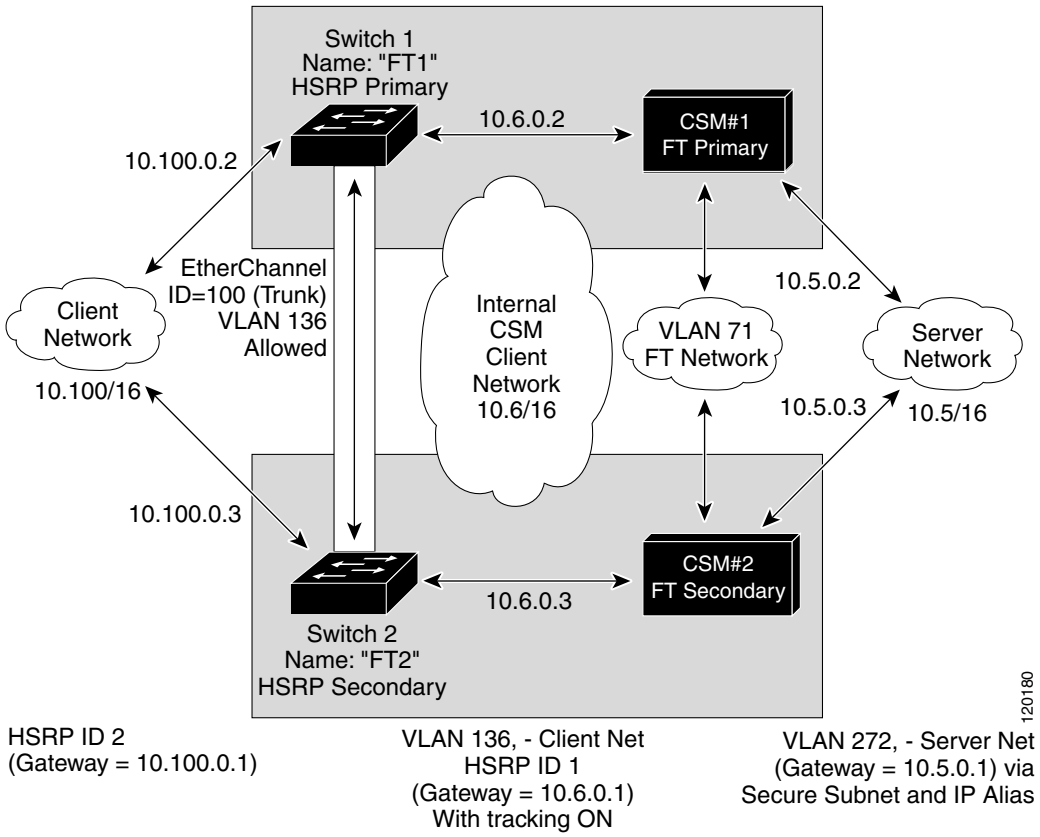
- Server VLAN 272

  The actual servers on the server network (10.5/1) point to the CSM server network through an aliased 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 client network to travel between the two Catalyst 6500 series switches. The setup is shown in Figure 7-2.

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

Figure 7-2 HSRP Configuration



Creating the HSRP Gateway

This procedure 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, follow 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, follow 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)# vlan 71

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
ip address 10.6.0.2 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
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)# vlan 71
```

```
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
ip address 10.6.0.3 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
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 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 Connection Redundancy

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

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` *virtserver-name*	Identifies a virtual server and enters the virtual server submode.

	Command	Purpose
Step 4	`Router(config-slb-vserver)# virtual ip-address [ip-mask] protocol port-number [service ftp]`	Configures the virtual server attributes.
Step 5	`Router(config-slb-vserver)# serverfarm serverfarm-name`	Associates a server farm with a virtual server.
Step 6	`Router(config-slb-vserver)# sticky duration [group group-id] [netmask ip-netmask]`	Ensures that connections from the same client use the same real server.
Step 7	`Router(config-slb-vserver)# replicate csrp sticky`	Enables sticky replication.
Step 8	`Router(config-slb-vserver)# replicate csrp 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 group group-id vlan vlanid`	Configures fault tolerance and enters the fault-tolerance submode.
Step 11	`Router(config-slb-ft)# priority value`	Sets the priority of the CSM.
Step 12	`Router(config-slb-ft)# failover failover-time`	Sets the time for a standby CSM to wait before becoming an active CSM.
Step 13	`Router(config-slb-ft)# preempt`	Allows a higher priority CSM 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
```

Configuring a Hitless Upgrade

A *hitless upgrade* allows you to upgrade to a new version without any 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 standby.

Step 3 Upgrade the standby system with the new release, and then reboot the CSM.

The standby CSM boots as standby with the new release. If you have sticky backup enabled, keep the standby CSM in standby mode for at least 5 minutes.

Step 4 Upgrade the active CSM.

Step 5 Reboot the active CSM.

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

Step 6 The rebooted CSM comes up as standby.