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 Connection Redundancy, page 9-8
- Configuring a Hitless Upgrade, page 9-9

Configuring Fault Tolerance

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

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 IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM-S is configured identically. The network sees the fault-tolerant configuration as a single CSM-S.

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.

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 modules connected to the same client-side and server-side VLANs.
- Communication between the CSM-S modules provided by a shared private VLAN.
- 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:

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

Because each CSM-S has a different 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 passive 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:

```
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 9-1* shows how the secure (router) mode fault-tolerant configuration is set up.
Figure 9-1  Fault-Tolerant Configuration

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config-module-csm)# vlan 2 client</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-slb-vlan-client)# gateway 192.158.38.20</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-module-csm)# vserver vip1</td>
</tr>
</tbody>
</table>
To configure the standby (B) CSM-S for fault tolerance, perform this task (see Figure 9-1):

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Router(config-slb-vserver)# virtual 192.158.38.30 tcp www</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-module-csm)# inservice</td>
</tr>
<tr>
<td>Step 7</td>
<td>Router(config-module-csm)# vlan 3 server</td>
</tr>
<tr>
<td>Step 8</td>
<td>Router(config-slb-vlan-server)# ip addr 192.158.39.10 255.255.255.0</td>
</tr>
<tr>
<td>Step 9</td>
<td>Router(config-slb-vlan-server)# alias ip addr 192.158.39.20 255.255.255.0</td>
</tr>
<tr>
<td>Step 10</td>
<td>Router(config-slb-vlan-server) vlan 9</td>
</tr>
<tr>
<td>Step 11</td>
<td>Router(config-module-csm)# ft group ft-group-number vlan 9</td>
</tr>
<tr>
<td>Step 12</td>
<td>Router(config-module-csm)# vlan</td>
</tr>
<tr>
<td>Step 13</td>
<td>Router(vlan)# vlan 2</td>
</tr>
<tr>
<td>Step 14</td>
<td>Router(vlan)# vlan 3</td>
</tr>
<tr>
<td>Step 15</td>
<td>Router(vlan)# vlan 9</td>
</tr>
<tr>
<td>Step 16</td>
<td>Router(vlan)# exit</td>
</tr>
</tbody>
</table>

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.
Chapter 9 Configuring Redundancy

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 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-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.

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

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu’s top level.
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)# 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 FastEthernet3/6 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
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# no ip igmp snooping</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-module-csm)# vserver virtserver-name</td>
</tr>
</tbody>
</table>
### Configuring Redundancy

#### 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 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.