CHAPTER 4

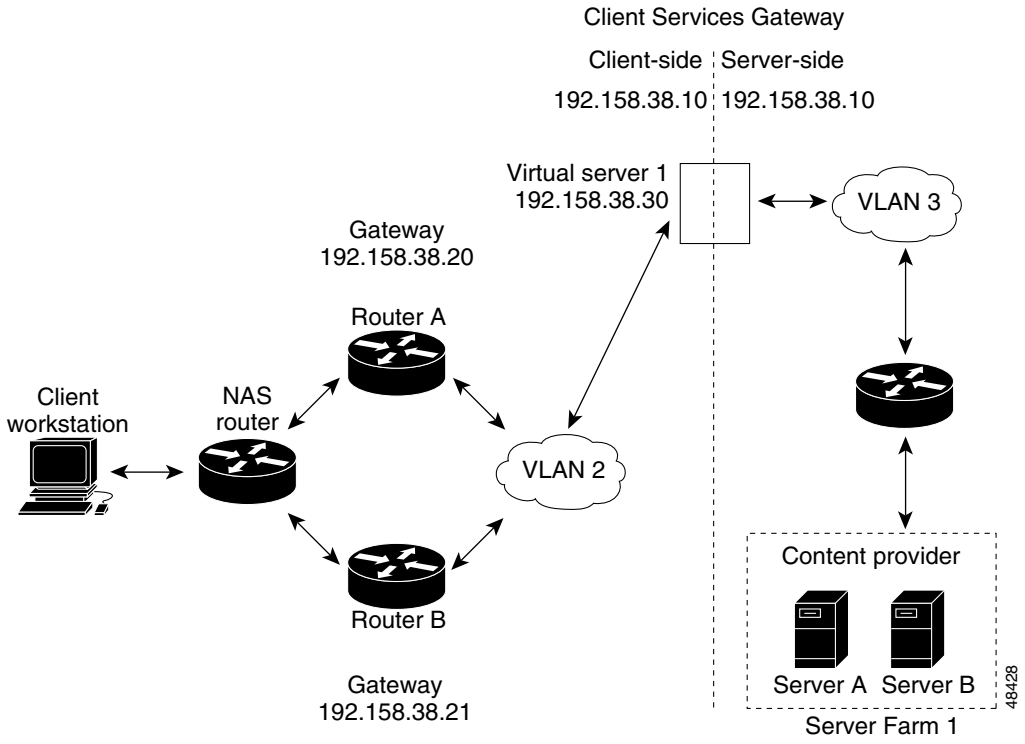
Configuring Secure (Router) Mode, Redundancy, Fault Tolerance, and HSRP

This chapter describes how to configure some aspects of content switching that are necessary for the Content Services Gateway to function properly. This information is contained in the following sections:

Configuring the Single Subnet (Bridge) Mode

In a single subnet (bridge) mode configuration, the client-side and server-side VLANs are on the same subnets. Figure 4-1 illustrates a typical single subnet (bridge) mode configuration.

Figure 4-1 Single Subnet (Bridge) Mode Configuration



To configure single subnet (bridge) mode content switching, first configure a client-side VLAN and a server-side VLAN, using the following procedure:

	Command	Purpose
Step 1	`Router# vlan database`	Enters the VLAN configuration mode.
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN.
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.

After you have configured a client-side VLAN and a server-side VLAN, assign the same IP address to the VLANs, using the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters module CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.
Step 3	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 4	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN 3 and enters the CSG VLAN server configuration mode.
Step 5	`Router(config-csg-vlan-server)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 3.

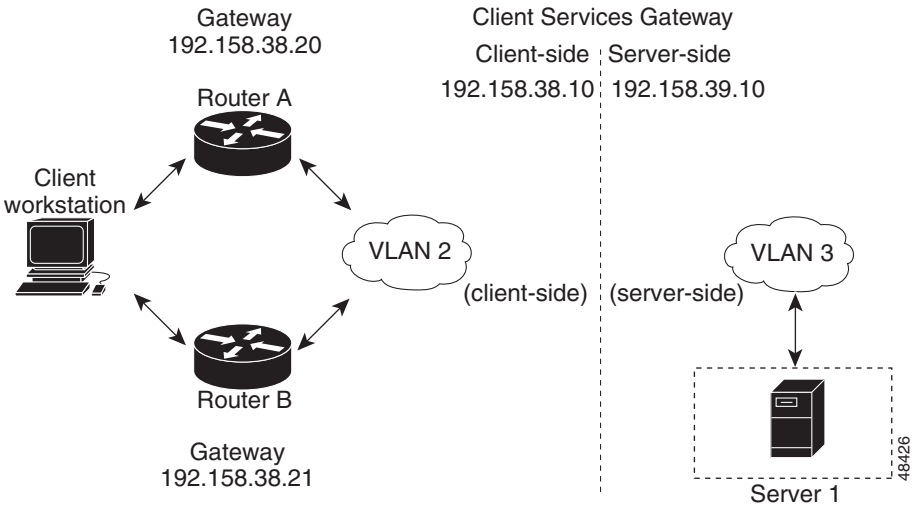
	Command	Purpose
Step 6	`Router(config-csg-vlan-server)# exit`	Exits the configuration mode.
Step 7	`Router(config-module-csg)# vserver VIP1`	Creates a virtual server and enters the CSG virtual server mode.

After you have assigned the IP addresses, set the server's default routes to Server A's gateway (192.158.38.20) or Server B's gateway (192.158.38.21).

Configuring the Secure (Router) Mode

Because the client-side and server-side VLANs are on different subnets, you can configure the CSG to operate in a secure (router) mode. Figure 4-2 shows how to set up the secure (router) mode configuration.

Figure 4-2 Secure (Router) Mode Configuration



To configure content switching in secure (router) mode, first configure a client-side VLAN and a server-side VLAN, using the following procedure:

	Command	Purpose
Step 1	`Router# vlan database`	Enters the VLAN configuration mode.
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN.
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.

After you have configured a client-side VLAN and a server-side VLAN, assign IP addresses to the VLANs, using the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters module CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.
Step 3	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 4	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN 3 and enters the CSG VLAN server configuration mode.
Step 5	`Router(config-csg-vlan-server)# ip address 192.158.39.10 255.255.255.0`	Assigns the CSG IP address on VLAN 3.

Configuring Fault Tolerance

This section describes a fault-tolerant (FT) configuration. In this configuration, two separate Catalyst 6000 series chassis each contain a CSG. The configuration can also apply to two separate Cisco 7600 series router chassis containing CSGs.

Note You can also create a fault-tolerant configuration with two CSGs in a single Catalyst 6000 series switch or Cisco 7600 series router chassis. You can create a fault-tolerant configuration in the secure (router) mode.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSG and the routers on the client side and the servers on the server side. In a redundant configuration, two CSGs perform active and standby roles. Each CSG contains the same IP, virtual server, and server farm. From the client-side and server-side networks, each CSG is configured identically. The network sees the fault-tolerant configuration as a single CSG.

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

If you have a pair of CSG cards and a pair of Content Services Module (CSM) cards in your network, *do not* configure both the CSG pair and the CSM pair to use the same FT VLAN. Use a different FT VLAN for each pair. If you configure the CSG pair and the CSM pair to use the same FT VLAN, then either service, the CSG or the CSM, is down in the standby mode.

Configuring fault-tolerance requires the following:

- Two CSGs that are installed in the Catalyst 6000 series switch or Cisco 7600 series router chassis.
- Identically configured CSGs. One CSG is negotiated at run time to be the active; the other is negotiated to be the standby.
- Each CSG connected to the same client-side and server-side VLANs.
- Communication between the CSGs provided by a shared private VLAN.
- A network that sees the redundant CSGs 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 CSG 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
```

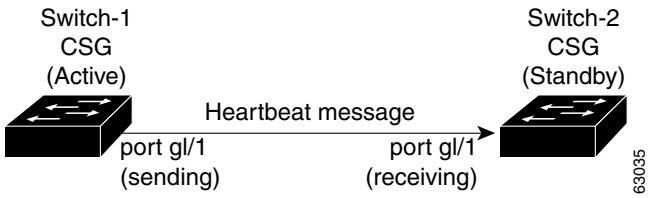
- Quality of service (QoS) configured on each CSG in the fault-tolerant pair with Cisco IOS Release 12.1(12c)E and later. Table 4-1 lists the QoS requirements.

Table 4-1 QoS Enabling Matrix

CSG Release	Cisco IOS Release	Supervisor Engine/MSFC	Configure QoS?
3.1(1)C3(1)	12.1(12c)E	SUP1-MSFC2	No
3.1(1)C3(1)	12.1(12c)E	SUP2-MSFC2	Yes
3.1(1)C4(1)	12.1(12c)E	SUP2-MSFC2	Yes
3.1(3)C5(1)	12.2(14)ZA7	SUP2-MSFC2	Yes
3.1(3)C5(5)	12.2(18)SXD	SUP720-MSFC3-BXL or SUP2-MSFC2	Yes

Figure 4-3 shows the QoS configuration topology.

Figure 4-3 QoS Configuration Topology



Without the secure (router) mode configuration shown in Figure 4-2, 802.1Q priority information is not preserved in packets traversing to the switch. Heartbeat messages sent from the active to the standby CSG must contain this priority information so that they are transmitted without delay. When an excessive delay occurs, an unnecessary takeover might occur.

You can overcome this limitation by configuring the sending port g1/1 to retain priority information upon transmission and the receiving port g1/1 to trust the class of service (CoS) (priority bits) for the incoming packets.

Configure the switch with the **permit any any** command to enable it to accept incoming packets with any MAC address from any MAC address.

To configure QoS for a fault-tolerant configuration, enter these commands:

```
Router(config)# mls qos
Router(config)# interface g1/1
Router(config-if)# no shutdown
Router(config-if)# mls qos cos 7
Router(config-if)# switchport
Router(config-if)# switchport access vlan 200
Router(config-if)# switchport trunk encapsulation dot1q
```

```
Router(config-if)# switchport trunk allowed vlan 1,2,1002-1005
Router(config-if)# switchport mode trunk
```

Table 4-2 lists CSG fault-tolerant configuration requirements.

Table 4-2 The CSG Fault-Tolerant Configuration Requirements

Configuration Parameter	On Both CSG Modules	
	Same	Different
VLAN name	X	
VLAN address		X
Gateway[1] address	X	
Content name	X	
Content IP address	X	
Alias IP addresses	X	
Redundancy group name	X	
Redundancy VLAN ID	X	

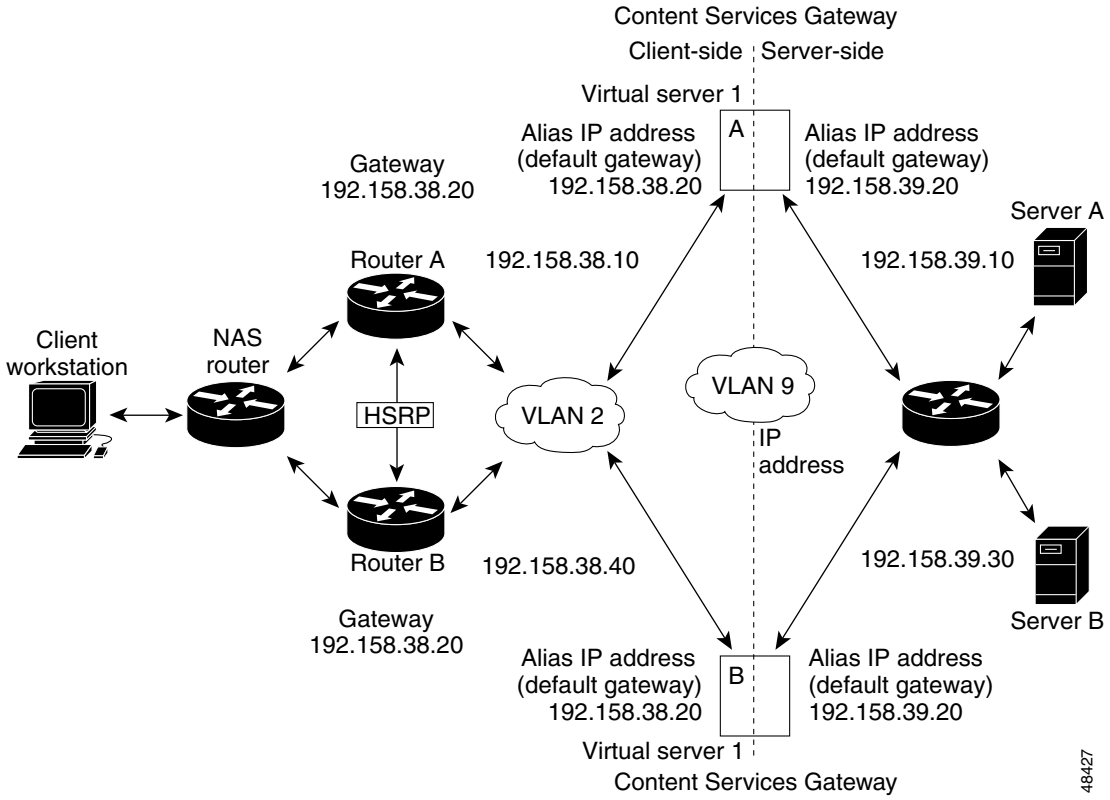
1. Server default gateways must point to the alias IP address.

Enter the **replicate connection tcp** command in content configuration mode to configure replication for the CSGs. (The default setting for the **replicate** command is disabled.)

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

Figure 4-4 shows how to set up a secure (router) mode fault-tolerant configuration.

Figure 4-4 Fault-Tolerant Configuration



To configure the active (A) CSG for fault tolerance, use the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.10 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 3	`Router(config-csg-vlan-client)# alias 192.158.38.30 255.255.255.0`	Assigns an alias address to the CSG.
Step 4	`Router(config-csg-vlan-client)# gateway 192.158.38.20 255.255.255.0`	(Optional) Defines the client-side VLAN gateway for an HSRP enabled gateway.
Step 5	`Router(config-module-csg)# ip csg content content1`	Creates a CSG content definition and enters the CSG content configuration mode.
Step 6	`Router(config-csg-content)# ip any tcp www`	Defines Layer 3/Layer 4 parameters of the content.
Step 7	`Router(config-csg-content)# inservice`	Enables the server.
Step 8	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 9	`Router(config-csg-vlan-server)# ip address 192.158.39.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.

	Command	Purpose
Step 10	`Router(config-csg-vlan-server)# alias 192.158.39.20 255.255.255.0`	Assigns an alias address to the CSG.
Step 11	`Router(config-module-csg) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 12	`Router(config-module-csg)# ft group` *ft-group-number* `vlan 9`	Enters fault-tolerant configuration mode and configures fault tolerance.
Step 13	`Router(config-module-csg)# end`	Ends module CSG configuration mode.
Step 14	`Router# vlan database`	Enters VLAN configuration mode.
Step 15	`Router(vlan)# vlan 2`	Configures a client-side VLAN 2.
Step 16	`Router(vlan)# vlan 3`	Configures a server-side VLAN 3.
Step 17	`Router(vlan)# vlan 9`	Configures a fault-tolerant VLAN 9.
Step 18	`Router(vlan)# exit`	Exits. The configuration takes affect.

To configure the standby (B) CSG for fault tolerance, perform this task (see Figure 4-4):

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.40 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 3	`Router(config-module-csg) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 4	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway.
Step 5	`Router(config-module-csg)# ip csg content content1`	Creates a CSG content definition and enters the CSG content configuration mode.
Step 6	`Router(config-csg-content)# ip any tcp www`	Defines Layer 3/Layer 4 parameters of the content.
Step 7	`Router(config-csg-vserver)# inservice`	Enables the server.
Step 8	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 9	`Router(config-csg-vlan-server)# ip address 192.158.39.30 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 10	`Router(config-csg-vlan-server)# alias 192.158.39.20 255.255.255.0`	Assigns an alias address to the CSG.
Step 11	`Router(config-module-csg)# ft group` *ft-group-number* `vlan 9`	Enters fault-tolerant configuration mode and configures fault tolerance.
Step 12	`Router(config-module-csg)# show module csg ft`	Displays the state of the fault tolerant system.

To configure fault tolerance in module CSG configuration mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csg)# ft group` *group-id* `vlan` *vlanid*	Configures fault tolerance and enters fault-tolerance configuration mode.
Step 2	`Router(config-csg-ft)# priority` *value*	Sets the priority of the CSG.
Step 3	`Router(config-csg-ft)# failover` *failover-time*	(Optional) Sets the time for a standby CSG to wait before becoming an active CSG.
Step 4	`Router(config-csg-ft)# heartbeat-time` *heartbeat-time*	(Optional) Sets the time before heartbeat messages are transmitted by the CSG.

This example shows how to set fault tolerance for connection redundancy in module CSG configuration mode:

```
Router(config-module-csg)# ft group 90 vlan 111
Router(config-csg-ft)# priority 10
Router(config-csg-ft)# failover 3
Router(config-cag-ft)# heartbeat-time 2
```

Configuring HSRP

This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see Figure 4-5) and describes how to configure the CSGs with HSRP and failover on the Catalyst 6000 series switches.

HSRP Configuration Overview

Figure 4-5 shows that two Catalyst 6000 series switches, Switch 1 and Switch 2, are configured to route from a client-side network (10.100/16) to an internal CSG 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 CSG 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 CSGs (one in Switch 1 and one in Switch 2) are configured to forward traffic between a client-side and a server-side VLAN:

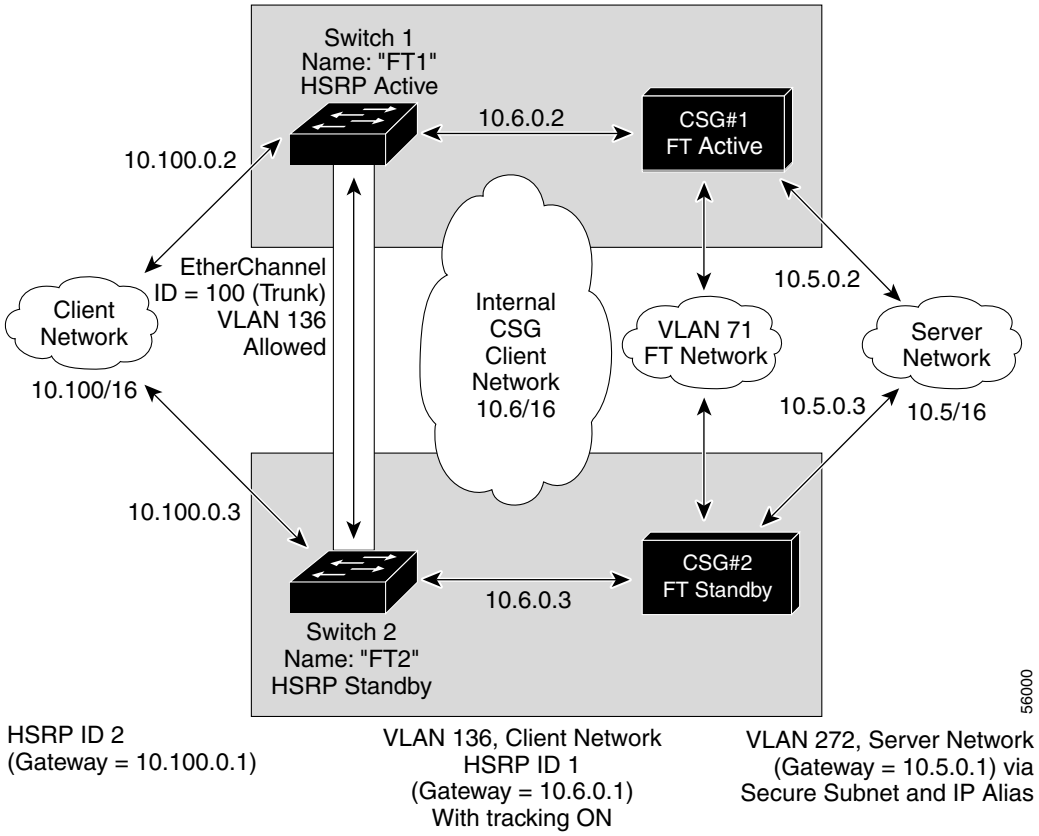
- Client VLAN 136 (The client VLAN is actually an internal CSG VLAN network; the actual client network is on the other side of the switch.)
- Server VLAN 272

The actual servers on the server network point to the CSG 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 CSG client network to travel between the two Catalyst 6000 series switches.

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

Figure 4-5 HSRP Configuration



Creating the HSRP Gateway

The following procedure describes how to create an HSRP gateway for the client-side network. The gateway is HSRP ID 2 for the client-side network. 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
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
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 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 csg 5
Router(config-module-csg)# vlan 136 client
Router(config-csg-vlan-client)# ip address 10.6.0.245 255.255.0.0
Router(config-csg-vlan-client)# gateway 10.6.0.1
Router(config-csg-vlan-client)# exit

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

Router(config-module-csg)# vlan 71 ft

Router(config-module-csg)# ft group 88 vlan 71
Router(config-csg-ft)# priority 30
Router(config-csg-ft)# exit

Router(config-module-csg)# interface Vlan136
ip address 10.6.0.2 255.255.0.0
standby 1 priority 100
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 csg 6
Router(config-module-csg)# vlan 136 client
Router(config-csg-vlan-client)# ip address 10.6.0.246 255.255.0.0
Router(config-csg-vlan-client)# gateway 10.6.0.1
Router(config-csg-vlan-client)# exit

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

Router(config-module-csg)# vlan 71 ft
Router(config-module-csg)# ft group 88 vlan 71
Router(config-csg-ft)# priority 20
```

```
Router(config-csg-ft)# exit

Router(config-module-csg)# interface Vlan136
ip address 10.6.0.3 255.255.0.0
standby 1 priority 100
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

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 (Optional) To prevent problems, remove the server and the FT CSG 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 hanging when the active CSG fails and the standby CSG becomes active. With connection redundancy, the active CSG replicates forwarding information to the standby CSG for each connection that is to remain open when the active CSG fails over to the standby CSG.

The CSG also supports stateful redundancy for TCP connections. That is, the session continues to be billed even when the primary CSG fails and the backup CSG takes over.

Stateful redundancy is not supported for RTSP connections. For all other connections, a new session is created when the backup CSG becomes active.

To configure connection redundancy, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip csg content` *content-name*	Defines content for CSG accounting services, and enters CSG content configuration mode.
Step 2	`Router(config-csg-content)# ip` *ip-address* [*ip-mask*] *protocol port-number*	Defines the Layer 3/Layer 4 flows that can be processed by the CSG accounting services.
Step 3	`Router(config-csg-content)# replicate connection tcp`	Replicates the connection state for all TCP connections to the CSG content servers on the backup system.
Step 4	`Router(config-csg-content)# inservice`	Enables the content definition.

This example shows how to configure connection redundancy:

```
Router(config)# ip csg content CISCO
Router(config-csg-content)# ip 10.10.10.10 tcp telnet
Router(config-csg-content)# replicate connection tcp
Router(config-csg-content)# inservice
```