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

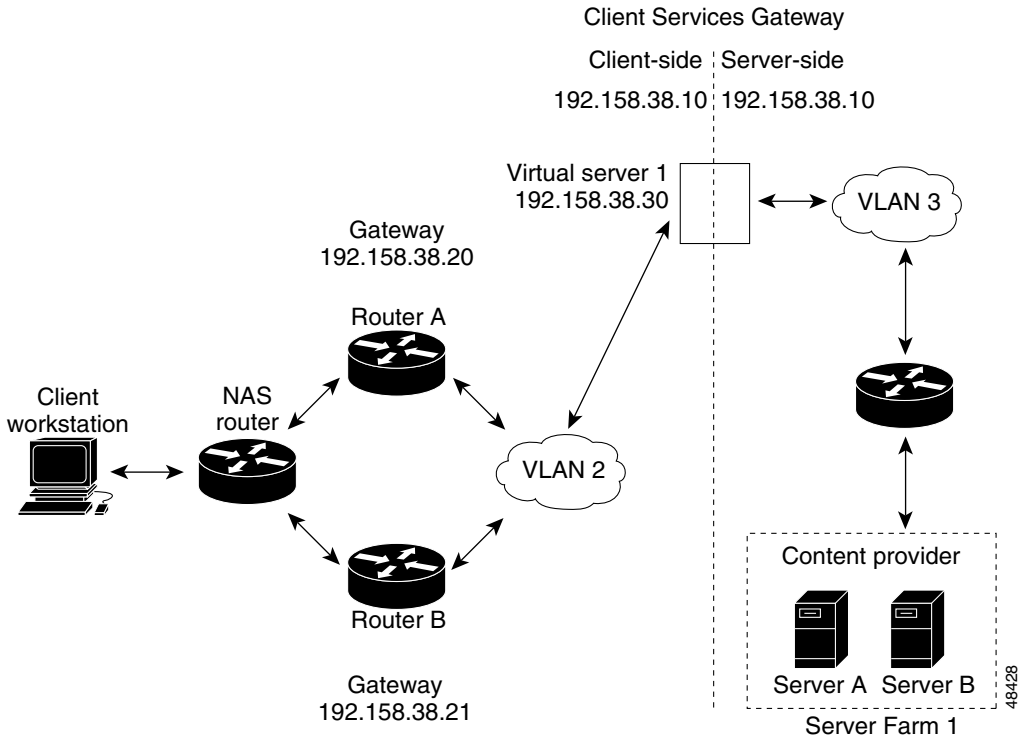
This chapter describes how to configure the following aspects of content switching that are necessary for the Content Services Gateway (CSG) to function properly:



## 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 shows 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 by following these steps:

| | 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 configure a client-side VLAN and a server-side VLAN, assign the same IP address to the VLANs by following these steps:

| | 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 192.158.38.10 255.255.255.0` | Assigns the CSG IP address on VLAN 3. |

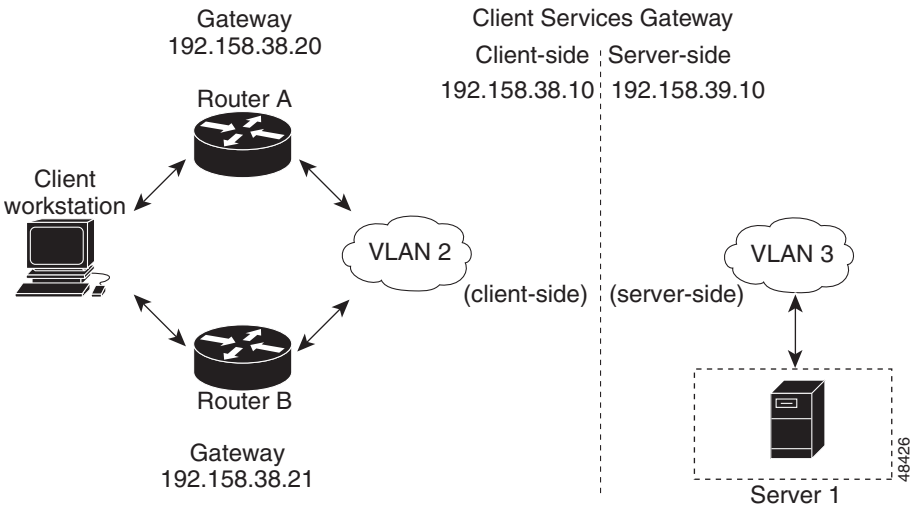
| | Command | Purpose |
|---|---|---|
| **Step 6** | `Router(config-csg-vlan-server)# exit` | Exits the configuration mode. |
| **Step 7** | `Router(config-module-csg)# vserver VIP1` | Creates a virtual server and enters the CSG virtual server mode. |

After you assign the IP addresses, set the server default routes to the Server A gateway (192.158.38.20) or the Server B 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 a 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 by following these steps:

| | 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 configure a client-side VLAN and a server-side VLAN, assign the same IP address to the VLANs by following these steps:

| | 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 192.158.38.10 255.255.255.0` | 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. This configuration can also be applied to two separate Cisco 7600 series router chassis containing CSGs.

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

In the secure (router) mode, the client-side and server-side VLANs provide the FT (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 is configured with the same IP, virtual server, and server farm. In both of the networks, the CSGs are configured identically. The network sees the FT configuration as a single CSG.

Configuring fault-tolerance requires the following conditions:

- Two CSGs are installed in a Catalyst 6000 series switch or a Cisco 7600 series router chassis.
- These two CSGs are identically configured CSGs. One CSG is negotiated at run time to be the active CSG; the other is negotiated to be the standby CSG.
- Both CSGs are connected to the same client-side and server-side VLANs.
- Communication between the CSGs is provided by a shared private VLAN.
- Each FT CSG pair must use a different FT VLAN.
- If you have pairs of CSG cards and pairs of CSM cards in your network, each pair must use a different FT VLAN. Do not configure a CSG pair and a CSM pair to use the same FT VLAN.
- The CSG does support trunked FT VLANs, but each pair of CSGs must use a unique FT VLAN and a unique group ID. In addition, make sure that the number of high availability messages between all pairs of CSGs on the trunk does not overwhelm the CSG card.
- The network sees the redundant CSGs as a single entity.

- Connection redundancy is provided by configuring a link that has a capacity of 1 GB per second. Enable the calendar in the switch Cisco IOS software so that the CSG state change is stamped with the correct time.

  To enable the calendar, enter these commands:

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

**Note** The CSG reports all times in Coordinated Universal Time (UTC), regardless of the setting of the **clock timezone** or **clock summer-time** command.

Table 4-1 lists CSG FT configuration requirements.

***Table 4-1 The CSG FT Configuration Requirements***

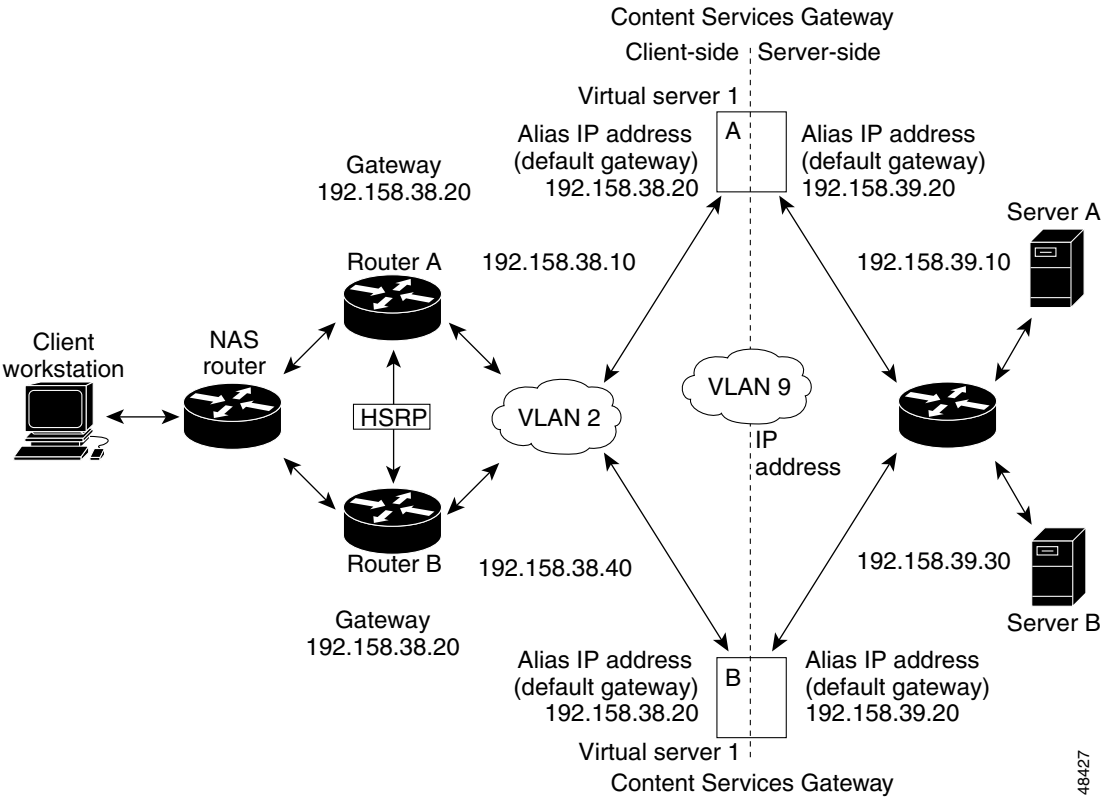
| | On Both CSG Modules | |
|---|---|---|
| **Configuration Parameter** | **Same** | **Different** |
| VLAN name | X | |
| VLAN address | | X |
| Gateway address (Server default gateways must point to the alias IP address.) | X | |
| Content name | X | |
| Content IP address | X | |
| Alias IP addresses | X | |
| Redundancy group name | X | |
| Redundancy VLAN ID | X | |

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

Figure 4-3 shows a secure (router) mode FT configuration.

***Figure 4-3 FT Configuration***




To configure the active (A) CSG for fault tolerance, follow these steps:

| | 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` | Configures a CSG content and enters the CSG content configuration mode. |
| **Step 6** | `Router(config-csg-content)# ip any tcp www` | Defines Layer 3 and Layer 4 parameters of the content. |
| **Step 7** | `Router(config-csg-content)# inservice` | Activates the content service on each CSG. |
| **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. |

| | Command | Purpose |
|---|---|---|
| **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. |
| **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 an FT VLAN. |
| **Step 12** | `Router(config-module-csg)# ft group` *ft-group-number* `vlan 9` | Enters FT 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 an FT VLAN 9. |
| **Step 18** | `Router(vlan)# exit` | Exits. The configuration takes effect. |

To configure the standby (B) CSG for fault tolerance, follow these steps (see Figure 4-3):

| | 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 an FT 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` | Configures a CSG content and enters the CSG content configuration mode. |
| **Step 6** | `Router(config-csg-content)# ip any tcp www` | Defines Layer 3 and 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 FT configuration mode and configures fault tolerance. |
| **Step 12** | `Router(config-module-csg)# show module csg ft` | Displays the state of the FT system. |

To configure fault tolerance in module CSG configuration mode, follow these steps:

| | 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, in seconds, 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, in seconds, 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-csg-ft)# heartbeat-time 2
```

# Configuring HSRP

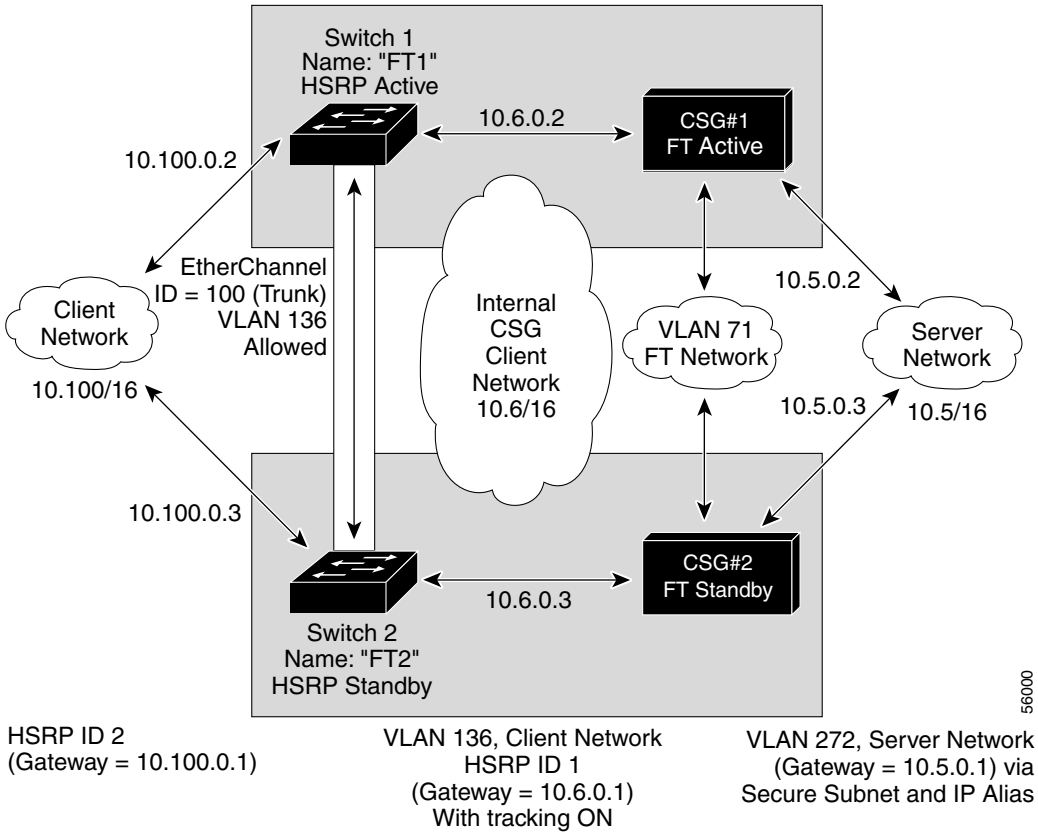
This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see Figure 4-4) and describes how to configure the CSGs with HSRP and failover on the Catalyst 6000 series switches.

## HSRP Configuration Overview

Figure 4-4 shows two Catalyst 6000 series switches, switch 1 and switch 2, that 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.

*Figure 4-4 HSRP Configuration*




**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 client network 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 VLAN and a server-side VLAN:

- Client VLAN 136 (The client VLAN is 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 configuration example, an EtherChannel is set up with trunking enabled, to allow 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 an active CSG in another switch, allowing independent failover of the CSGs and switches, providing an extra level of fault tolerance.

# Creating the HSRP Gateway

In the following procedure, an HSRP gateway is created 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 port 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 FT HSRP Configurations

This section describes how to create an FT HSRP secure mode configuration. To create a nonsecure mode configuration, enter the commands described in this example, with these exceptions:

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

To create FT HSRP configurations, follow these steps:

**Step 1** Configure the 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 the 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 becoming unresponsive 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.

To configure connection redundancy, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip csg content content-name` | Configures 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 and 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 standby system. |
| **Step 4** | `Router(config-csg-content)# inservice` | Enables the content configuration. |

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
```

To specify that sessions are to be replicated only if configured in the content, enter the following command in module CSG configuration mode:

```
Router(config-csg-module)# variable CSG_FT_CONTENT 1
```

To specify that sessions are always to be replicated (the default setting), enter the following command in module CSG configuration mode:

```
Router(config-csg-module)# variable CSG_FT_CONTENT 0
```

To specify the delay, in sixtieths of a second, after sending FTP content information to the standby, enter the following command in module CSG configuration mode:

```
Router(config-csg-module)# variable CSG_FTP_HA_WAIT_DELAY delay
```

To specify the delay, in seconds, before replicating session information, enter the following command in module CSG configuration mode:

```
Router(config-csg-module)# variable CSG_FT_SESSION_DELAY delay
```

For more information about these variables, see the description of the **variable (module csg)** command.