



# Networking with the Content Switching Module with SSL

---

This chapter describes networking the CSM-S and contains these sections:

- [Configuring Modes for Networking, page 2-1](#)
- [CSM-S Networking Topologies, page 2-4](#)
- [Routing with the CSM-S, page 2-7](#)
- [Protecting Against Denial-of-Service Attacks, page 2-8](#)

## Configuring Modes for Networking

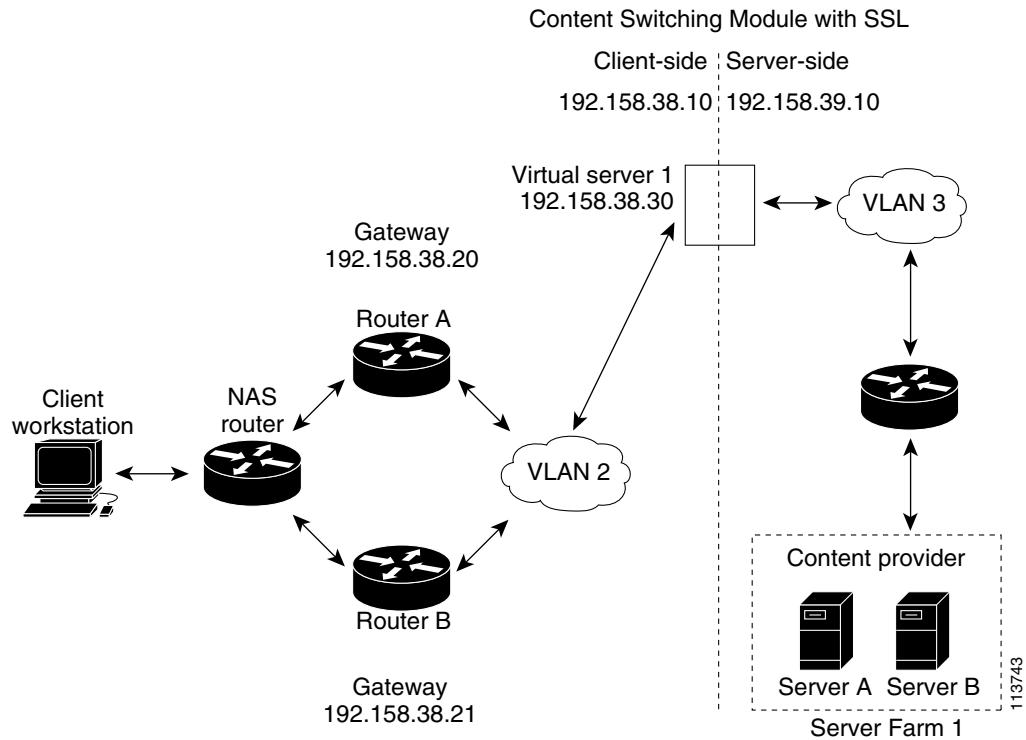
You can configure the CSM-S in a secure or router mode and a single subnet or bridged mode. These sections describe the modes:

- [Configuring the Secure \(Router\) Mode, page 2-1](#)
- [Configuring the Single Subnet \(Bridge\) Mode, page 2-3](#)

## Configuring the Secure (Router) Mode

In secure (router) mode, the client-side and server-side VLANs are on different subnets. [Figure 2-1](#) shows how the secure (router) mode configuration is set up.

Figure 2-1 Secure (Router) Mode Configuration

**Note**

The addresses in [Figure 2-1](#) refer to the steps in the following task table.

To configure content switching in secure (router) mode, perform this task:

	Command	Purpose
<b>Step 1</b>	Router(config-module-csm)# <b>vlan database</b>	Enters the VLAN mode <sup>1</sup> .
<b>Step 2</b>	Router(vlan)# <b>vlan 2</b>	Configures a client-side VLAN <sup>2</sup> .
<b>Step 3</b>	Router(vlan)# <b>vlan 3</b>	Configures a server-side VLAN.
<b>Step 4</b>	Router(vlan)# <b>exit</b>	Exits the mode for the configuration to take effect.
<b>Step 5</b>	Router(config-module-csm)# <b>vlan 2 client</b>	Creates the client-side VLAN 2 and enters the SLB VLAN mode.
<b>Step 6</b>	Router(config-slb-vlan-client)# <b>ip addr 192.158.38.10 255.255.255.0</b>	Assigns the CSM-S IP address on VLAN 2.
<b>Step 7</b>	Router(config-slb-vlan-client)# <b>gateway 192.158.38.20</b>	Defines the client-side VLAN gateway to Router A.
<b>Step 8</b>	Router(config-slb-vlan-client)# <b>gateway 192.158.38.21</b>	Defines the client-side VLAN gateway to Router B.
<b>Step 9</b>	Router(config-module-csm)# <b>vlan 3 server</b>	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
<b>Step 10</b>	Router(config-slb-vlan-server)# <b>ip addr 192.158.39.10 255.255.255.0</b>	Assigns the CSM-S IP address on VLAN 3.
<b>Step 11</b>	Router(config-slb-vlan-server)# <b>exit</b>	Exits the submode.

	Command	Purpose
Step 12	Router(config-module-csm) # <b>vserver VIP1</b>	Creates a virtual server and enters the SLB virtual server mode.
Step 13	Router(config-slb-vserver) # <b>virtual 192.158.38.30 tcp www</b>	Creates a virtual IP address.
Step 14	Router(config-slb-vserver) # <b>serverfarm farm1</b>	Associates the virtual server with the server farm <sup>3</sup> .
Step 15	Router(config-module-csm) # <b>inservice</b>	Enables the server.

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.
3. This step assumes that the server farm has already been configured. (See the "Configuring Server Farms" section on page 5-1.)

**Note**

Set the server default routes to the CSM-S IP address (192.158.39.10).

## Configuring the Single Subnet (Bridge) Mode

In the single subnet (bridge) mode configuration, the client-side and server-side VLANs are on the same subnets.

**Note**

You configure single subnet (bridge) mode by assigning the same IP address to the CSM-S client and server VLANs.

**Note**

The addresses in [Figure 2-1](#) refer to the steps in the following task table, with the exception of setting the server-side IP address to the same value as the client-side IP address.

To configure content switching for the single subnet (bridge) mode, perform this task:

	Command	Purpose
Step 1	Router(config-module-csm) # <b>vlan database</b>	Enters the VLAN mode <sup>1</sup> .
Step 2	Router(vlan) # <b>vlan 2</b>	Configures a client-side VLAN <sup>2</sup> .
Step 3	Router(vlan) # <b>vlan 3</b>	Configures a server-side VLAN.
Step 4	Router(vlan) # <b>exit</b>	Exits the mode for the configuration to take effect.
Step 5	Router(config-module-csm) # <b>vlan 2 client</b>	Creates the client-side VLAN 2 and enters the SLB VLAN mode <sup>1</sup> .
Step 6	Router(config-slb-vlan-client) # <b>ip addr 192.158.38.10 255.255.255.0</b>	Assigns the CSM-S IP address on VLAN 2.
Step 7	Router(config-slb-vlan-client) # <b>gateway 192.158.38.20</b>	Defines the client-side VLAN gateway to Router A.
Step 8	Router(config-slb-vlan-client) # <b>gateway 192.158.38.21</b>	Defines the client-side VLAN gateway to Router B.

	Command	Purpose
Step 9	Router(config-slb-vserver)# <b>vlan 3 server</b>	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	Router(config-slb-vlan-client)# <b>ip addr 192.158.38.10 255.255.255.0</b>	Assigns the CSM-S IP address on VLAN 3.
Step 11	Router(config-slb-vlan-server)# <b>exit</b>	Exits the submode.
Step 12	Router(config-module-csm)# <b>vserver VIP1</b>	Creates a virtual server and enters the SLB virtual server mode.
Step 13	Router(config-slb-vserver)# <b>virtual 192.158.38.30 tcp www</b>	Creates a virtual IP address.
Step 14	Router(config-slb-vserver)# <b>serverfarm farm1</b>	Associates the virtual server with the server farm <sup>3</sup> .
Step 15	Router(config-module-csm)# <b>inservice</b>	Enables the server.

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.
3. This step assumes that the server farm has already been configured. (See the "Configuring Server Farms" section on page 5-1.)

**Note**

Set the server default routes to Router A gateway (192.158.38.20) or Router B gateway (192.158.38.21).

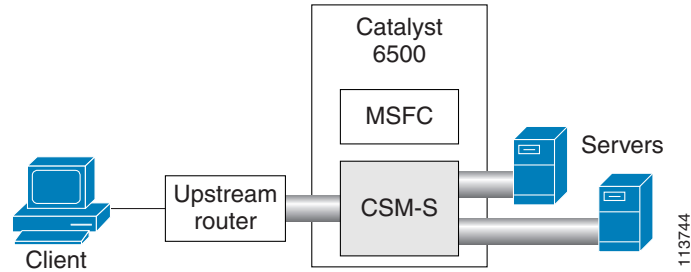
## CSM-S Networking Topologies

This section describes CSM-S networking topologies and contains these sections:

- [CSM-S Inline and MSFC Not Involved, page 2-4](#)
- [CSM-S Inline and MSFC on Server Side, page 2-5](#)
- [CSM-S Inline and MSFC on Client Side, page 2-5](#)
- [CSM-S in Aggregate Mode, page 2-6](#)
- [Direct Server Return, page 2-6](#)

### CSM-S Inline and MSFC Not Involved

[Figure 2-2](#) shows the CSM-S in a Layer 3 configuration without interaction with the MSFC.

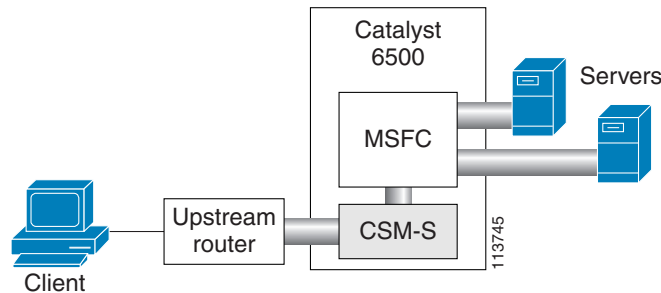
**Figure 2-2 CSM-S Inline, MSFC Not Involved**

This configuration has these characteristics:

- The MSFC is not routing CSM-S VLANs.
- All server-to-server communications (direct Layer 3 or load balanced) are through the CSM-S.
- The CSM-S must use static routes to the upstream router (default gateway).

## CSM-S Inline and MSFC on Server Side

Figure 2-3 shows the CSM-S in a configuration where the MSFC is located on the server side.

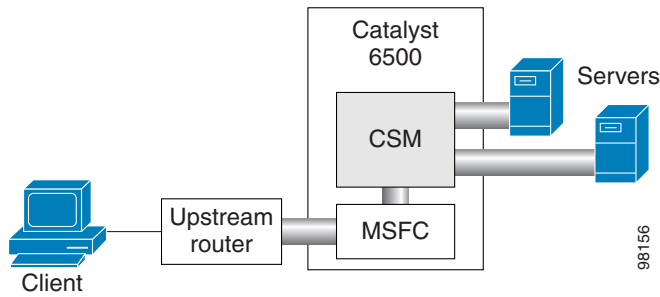
**Figure 2-3 CSM-S Inline, MSFC Located on Server Side**

This configuration has these characteristics:

- Server-to-server direct communications bypass the CSM-S.
- Server-to-server load-balanced connections always require secure NAT (SNAT).
- The CSM-S must use static routes to the upstream router (default gateway).
- Routing protocols can be used in the back end.
- Layer-2 rewrite is not possible.

## CSM-S Inline and MSFC on Client Side

Figure 2-4 shows the CSM-S in a configuration where the MSFC is located on the client side.

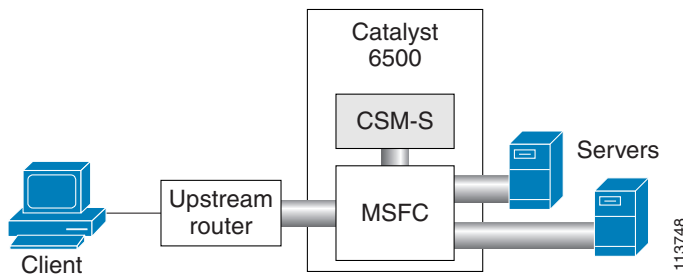
**Figure 2-4 CSM-S Inline, MSFC Located on the Client Side**

This configuration has these characteristics:

- The configuration is easy to deploy.
- Server-to-server Layer-3 communications pass through the CSM-S.
- Routing protocols can be used between the MSFC and the upstream router.
- All traffic to or from the servers passes through the CSM-S.

## CSM-S in Aggregate Mode

Figure 2-5 shows the CSM-S in an aggregate-mode configuration.

**Figure 2-5 CSM-S Located in Aggregate Mode**

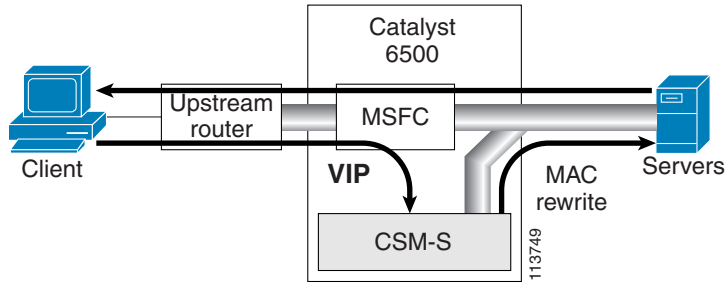
This configuration has these characteristics:

- The CSM-S is not inline, and the module does not see unnecessary traffic.
- Easy routing and CSM-S configuration.
- Requires PBR or client SNAT because return traffic is required.
- Server-to-server load-balanced connections always require SNAT.
- Layer-2 rewrite is not possible.

## Direct Server Return

Figure 2-6 shows the CSM-S in a direct server return configuration.

Figure 2-6 Direct Server Return



This configuration has these characteristics:

- High throughput or bandwidth is not required in the load balancer.
- The load balancer does not recognize return traffic.
- TCP flows always have to be timed out.
- TCP termination is not possible (only Layer 4 load balancing).
- Inband health monitoring is not possible.
- Servers must be Layer-2 adjacent with a loopback address.

## Routing with the CSM-S

When forwarding and maintaining load-balancing connections, the CSM-S must make routing decisions. However, the CSM-S does not run any routing protocols and does not have access to the MSFC routing tables. The CSM-S builds its own routing table with three types of entries:

- Directly attached IP subnets

These subnets are configured on the CSM-S client or the server VLANs.

- Default gateways

Default gateways are configured with the **gateway** keyword from within a client or server VLAN configuration submode. See [Chapter 4, “Configuring VLANs.”](#) In this release, you may have up to 511 default gateways. However, you cannot have more than seven default gateways for the same VLAN.

Most configurations have (or can be simplified to have) a single default gateway. This gateway points to the upstream router (or to an HSRP IP address that represents the upstream router pair) and eventually to various static routes.

- Static routes

Static routes are configured with the **route** keyword from within a client or server VLAN configuration submode of configuration. See [Chapter 4, “Configuring VLANs.”](#) Static routes are very useful when some servers are not Layer 2 adjacent.

Multiple default gateways are supported, however, they create a situation where if the CSM-S needs to make a routing decision to an unknown destination, the CSM-S will randomly select one of the gateways without your intervention or control. To control this behavior, use the predictor-forward option.

There are three situations in which the CSM-S must make a routing decision:

- Upon receiving a new connection.

At this time, the CSM-S decides where to send the return traffic for that connection. Unlike other devices, the CSM-S does not perform a route lookup, but it memorizes the source MAC address from where the first packet of the connection was received. Return traffic for that connection is sent back to the source MAC address. This behavior also works with redundancy protocols between upstream routers, such as HSRP.

- The CSM-S is configured in router mode.

The servers are pointing to the CSM-S as their default gateway, and the servers are originating connections.

- A server farm is configured with the predictor-forward option. (See [Chapter 5, “Configuring Real Servers and Server Farms.”](#)) This predictor instructs the CSM-S to route the connection instead of load balancing it.

With multiple gateways, the first two situations can be simplified by using a server farm configured with the gateway as a unique real server. (See the [“Configuring the Source NAT for Server-Originated Connections to the VIP”](#) section on page A-7.)

## Protecting Against Denial-of-Service Attacks

The CSM-S implements a variety of features to protect the devices that it is load balancing and to protect itself from a DoS attack. You cannot configure many of these features because they are controlled by the CSM-S and adjust to the amount of incoming traffic.

The CSM-S provides these DoS-protection features:

- SYN cookies




---

**Note** Do not confuse a SYN cookie with synchronization of cookies because these are different features. This discussion refers only to SYN cookies.

---

When the number of pending connections exceeds a configurable threshold, the CSM-S begins using SYN cookies, encrypting all of the connection state information in the sequence numbers that it generates. This action prevents the CSM-S from consuming any flow state for pending (not fully established) TCP connections. This behavior is fully implemented in hardware and provides a good protection against SYN attacks.

- Connection pending timeout

This feature is configurable on a per-virtual server basis and allows you to time out connections that have not been properly established within the configured timeout value specified in seconds.

- Connection idle timeout

This feature is configurable on a per-virtual server basis and allows you to time out established connections that have not been passing traffic for longer than an interval configured on a timer.

- Generic TCP termination

Some connections may not require TCP termination for Layer 7 load balancing. You can configure any virtual server to terminate all incoming TCP connections before load balancing those connections to the real servers. This configuration allows you to take advantage of all the CSM-S DoS features located in Layer 4 load-balancing environments.