CHAPTER 2

Networking with the Content Switching Module

The following sections describe networking the CSM:

Deployment Modes

You can configure the CSM in different deployment modes. Each of the modes supports different features and functionality, and each mode has its own advantages and caveats. This section describes each of the deployment modes, including the factors to consider in choosing the best mode for specific network requirements.

The deployment modes are described in the following subsections:

Single Subnet Bridge Mode

In single subnet bridge mode, the CSM acts as a Layer 2 device, bridging traffic flows between client and server VLANs. The CSM rewrites the destination MAC address. The client-side and server-side VLANs must exist on the same IP subnet.

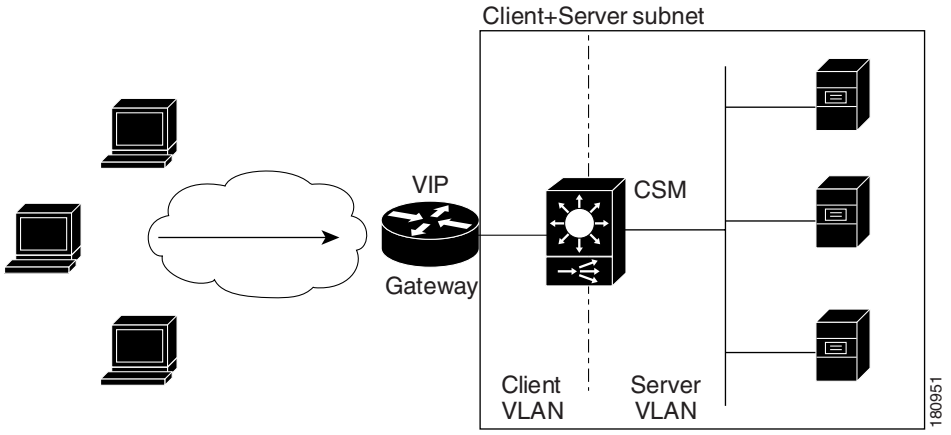
This is an inline mode (all traffic between the clients and the servers traverse the CSM).

Single subnet bridge mode is also known as transparent mode, because the CSM traffic handling is invisible to Layer 3 in this mode.

In this deployment mode, the CSM cannot act as the gateway for the servers. Typically, the MSFC is configured as the default gateway.

The following diagram displays a logical overview of the CSM operating in single subnet bridge mode.

Figure 2-1 CSM configured in Bridge Mode



Advantages

Bridge mode offers several advantages:

- Simpler configuration

  Because the CSM operates at layer 2, load balanced devices can be added to a network without disrupting the layer 3 network topology (no additional layer 3 hops are required).

- Full IOS feature set

  The MSFC, which runs full Cisco IOS software, provides the default gateway. You can use IOS features such as Hot Standby Router Protocol (HSRP) to support redundancy for the server default gateways.

- Direct Server Access

  The CSM bridges all non-VIP messages onto the server VLAN. This traffic includes management traffic directed to the real server IP addresses.

- Server originated traffic

  By default, the CSM bridges server-originated traffic to the server gateway (usually the MSFC), which does not require any special configuration.

- Multicast support

  Multicast support is automatic, because the MSFC is the default gateway

Cautions

When using bridge mode, be aware of the following cautions:

- Visibility of the real servers

  The real servers are visible to the client VLAN, because packets that don't match a VIP are still bridged onto the server VLAN. You may need to add extra configuration in the MSFC to ensure security of the servers.

- Server to server traffic

  The CSM does not bridge server to server traffic. This traffic is routed by the default gateway, and flows through the CSM in both directions. Therefore, server to server traffic consumes significant CSM resources in bridge mode.

Typical Usage:

Bridge mode is appropriate in a load balancing environment that you want to be transparent to Layer 3.

For example, many internet service providers use transparent cache redirection. You can put a CSM in between two routers and still have those 2 routers see each other as neighbors, running all sort of routing protocols. Meanwhile, the CSM can hijack traffic, even at L7, without disrupting the Layer 3 topology.

Bridge mode is also practical when replacing Local Director environments, as Local Director was a bridge device. Bridge mode is useful when introducing load balancing into an environment, as the number of IP changes is minimal.

You can easily implement multi-tier server farms using bridge mode. In this case, the CSM is configured with the VLAN for each tier and all servers use the FWSM (or the MSFC) as the default gateway. Access control lists (ACLs) can be deployed on the FWSM or the MSFC to limit server farm communications.

This configuration provides easy scalability and allows the use of a single CSM to be shared across the entire server farm. To keep the CSM from forwarding traffic between tiers and bypassing the FWSM, use the vlan keyword for each virtual server (vserver) configuration. This ensures that only traffic from the specified VLAN or VLANs is forwarded by the vserver.

Secure Router Mode

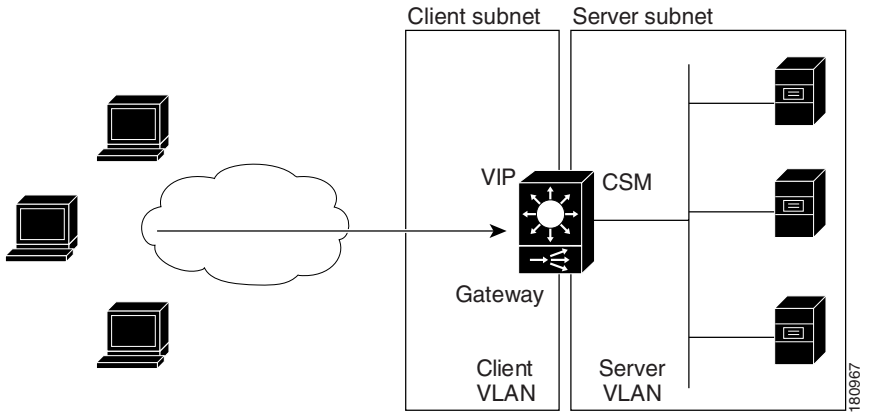
In secure router mode, the client side and server side VLANs are on different subnets. Therefore, the CSM acts as a Layer 3 device, routing traffic flows between clients and servers. The CSM rewrites the destination MAC address and the IP address.

This is an inline mode (all traffic between the client side and the servers traverse the CSM). This mode is also known as secure mode, as the servers are isolated in their own subnet. In this mode, the server default gateway is the CSM.

Support for high availability for the default gateway is through the alias command on the CSM. The alias command provides functionality very similar to HSRP by supplying a floating IP and a virtual MAC address which servers point to as the default gateway.

Figure 2-2 represents a logical overview of the CSM secure router mode.

Figure 2-2 CSM configured in Router Mode



Advantages

Secure router mode offers the following advantages:

- Security

  Only the VIP is visible to clients. The real server IP addresses are not reachable from the client subnetwork.

- Efficient server to server traffic

  The real servers are in there own subnet, so server to server traffic is Layer 2 switched.

- Flexible server farm configuration

  The real servers are not geographically constrained. Because the CSM is operating at Layer 3, it can reach servers anywhere on the network.

Cautions

When using router mode, be aware of the following cautions:

- CSM is not a full router

  The CSM does not offer the full IOS feature set.

- Redundancy

  You must use CSM redundancy instead of HSRP

- Direct Server Access

  You must define static routes in the CSM to provide direct access to the server subnet

Typical Usage

You can use router mode when you expect large volumes of traffic between the real servers.

You can use router mode when you want to isolate the real servers from hostile client attacks or if you want to distribute the real servers on a Layer 3 network.

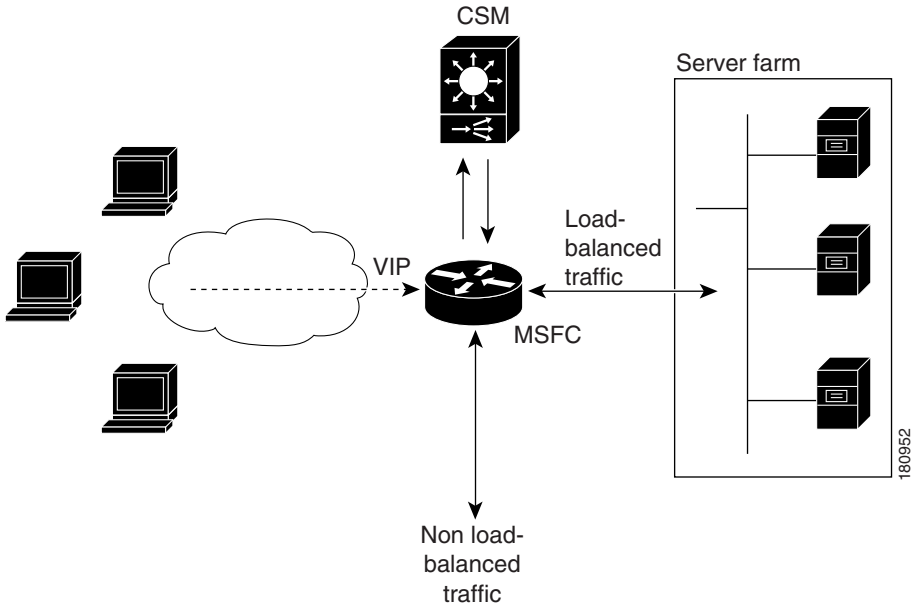
One-arm Mode

In one-arm mode, the CSM is configured as a single VLAN off the MSFC. The CSM is not inline between the clients and servers.

The real servers are connected to the MFSC (directly, or via intermediate routers).

The MSFC is configured to select which traffic flows to send through the CSM (for example, by using policy-based routing).

Figure 2-3 CSM configured in One Arm Mode



Advantages

One arm mode offers the following advantages:

- Efficient utilization of CSM resources, because non load-balanced traffic can bypass the CSM

Cautions:

When using one arm mode, be aware of the following cautions:

- You need to configure PBR or client SNAT to direct return traffic to the CSM.
- Server-to-server load-balanced connections always require SNAT.
- Layer 2 rewrite is not possible.

Typical Usage

One-arm design is useful where you have high throughput server-to-server traffic (for example, backup traffic) and with mainframes that require load balancing.

The one arm CSM mode provides a means for optimizing backend server-to-server communication. Often, servers residing in the data center need to communicate with each other or with databases residing within the data center. These communications do not necessarily need to be sent to the content switch for load balancing. This deployment mode utilizes policy based routing (PBR) to provide a means for configuring the Catalyst 6500 to only route certain traffic flows to the content switch, therefore alleviating unnecessary traffic flows from being forwarded to the content switch. The mode has other advantages as well. It allows you to configure the server default gateway on the MSFC allowing high availability to be provided by HSRP. It also allows you to use certain Cisco IOS features, such as Private VLANs, for the server farm.

Direct Server Return

Direct server return (DSR) is similar to one-arm mode, as the CSM is deployed off the MSFC. However, in this mode, all return traffic from the server bypasses the CSM.

In theory, this mode looks attractive, as the CSM is not loaded down with the return traffic. However, in reality, DSR has restrictions that limit its use in a real-world environment. For example, L7 features (like cookie stickiness) require return flows to pass through the CSM.

DSR has the following characteristics:

- Offloads the CSM, as the CSM does not process the return traffic.
- TCP flows always need 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.

CSM and MSFC Topologies

You can configure the CSM on the client side or server side of the MSFC. This section describes the advantages of each topology.

A significant consideration is that the MSFC runs full IOS, and therefore provides a full set of Layer 3 capabilities to the load balancing environment. The CSM provides only a subset of IOS capabilities.

With the CSM inline, the most common topology is to deploy MSFC on the client side. You can also deploy the MSFC on the server side, or you can bypass the MSFC completely. Reasons to consider these choices are described below.

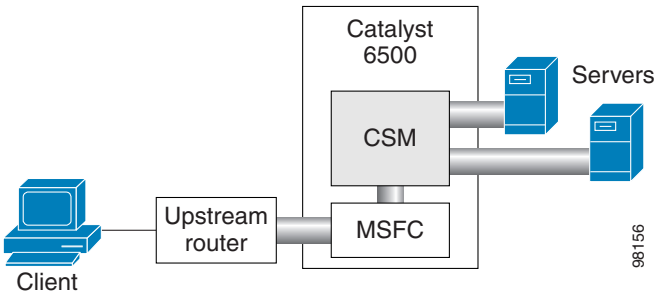
The following sections describe the CSM and MSFC topologies:

- CSM Inline and MSFC on Client Side, page 2-7
- CSM Inline and MSFC Not Involved, page 2-7
- CSM Inline and MSFC on Server Side, page 2-8
- CSM in One-arm mode, page 2-8

CSM Inline and MSFC on Client Side

The most common topology is with the CSM inline and located on the server side of the MSFC.

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



This configuration has the following benefits:

- The configuration is easy to deploy

  The upstream routers only need to know the VIP address. All other complexity is hidden behind the MSFC.

- Routing protocols can be used between the MSFC and the upstream router.

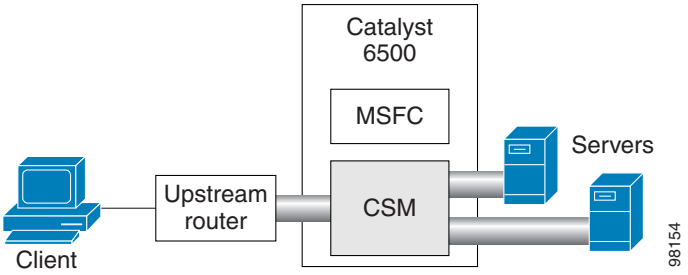
The following cautions

- All Server-to-server Layer 3 communications pass through the CSM.

CSM Inline and MSFC Not Involved

Figure 2-5 shows the CSM in a Layer 3 configuration without interaction with the MSFC.

Figure 2-5 CSM Inline, MSFC Not Involved



This configuration has the following characteristics:

- The MSFC is not routing CSM VLANs.
- All server-to-server communications (direct Layer 3 or load balanced) must go through the CSM to the upstream router and back through the CSM.
- The upstream router is the client gateway.

- The client VLAN starts at the upstream router

In Bridge Mode, this configuration has the following additional characteristics:

- You must configure a trunk from the upstream router to the Cat6K, to carry the VLAN information.

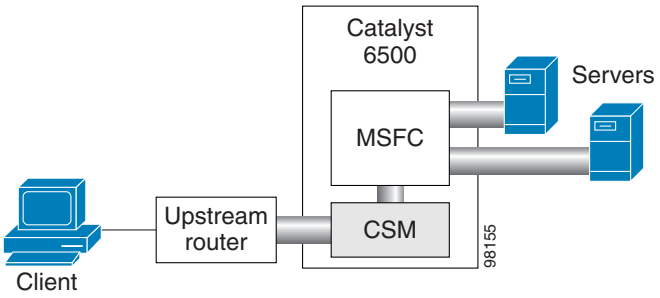
The main advantage of this topology is that the MSFC is off-loaded.

The main caveat is that the upstream router takes on extra responsibilities.

CSM Inline and MSFC on Server Side

Figure 2-6 shows the CSM in a configuration where the MSFC is located on the server side.

Figure 2-6 CSM Inline, MSFC Located on the Server Side



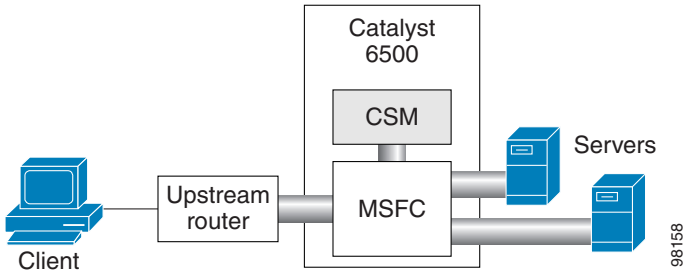
This configuration has the following characteristics:

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

CSM in One-arm mode

The MSFC must be on the client side when you configure the CSM in one-arm mode. See the "CSM in One-arm mode" section on page 2-8 for a description of this mode.

Figure 2-7 CSM in one-arm mode.



Routing with the CSM

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

- Directly attached IP subnets

  These subnets are configured on the CSM 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, if the CSM needs to make a routing decision to an unknown destination, the CSM will randomly select one of the gateways without your intervention or control. To control this behavior, use the predictor forward option described in the next paragraph.

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

- Upon receiving a new connection.

  At this time, the CSM needs to decide where to send the return traffic for that connection. Unlike other devices, the CSM will 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 is configured in router mode.

  The servers are pointing to the CSM 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 to route the connection instead of load balancing it.

In case of 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.

If the CSM receives a Layer 2 packet from a router for which the CSM does not have an ARP entry, the CSM does not send an ARP request to the router and the CMS drops the packet. However, if the CSM subsequently learns the router's ARP entry, the CSM processes packets from the router. This leads to inconsistent behavior when the ARP cache is cleared (for example, when the CSM is reloaded or fails over to a standby CSM).

Protecting Against Denial-of-Service Attacks

The CSM 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 and adjust to the amount of incoming traffic.

The CSM 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 begins using SYN cookies, encrypting all of the connection state information in the sequence numbers that it generates. This action prevents the CSM 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 DoS features located in Layer 4 load-balancing environments.

Configuring Deployment Modes

You can configure the CSM in bridged mode or router mode. The following sections describe the procedures for each of these modes:

- Configuring the Secure (Router) Mode, page 2-11
- Configuring the Single Subnet (Bridge) Mode, page 2-12

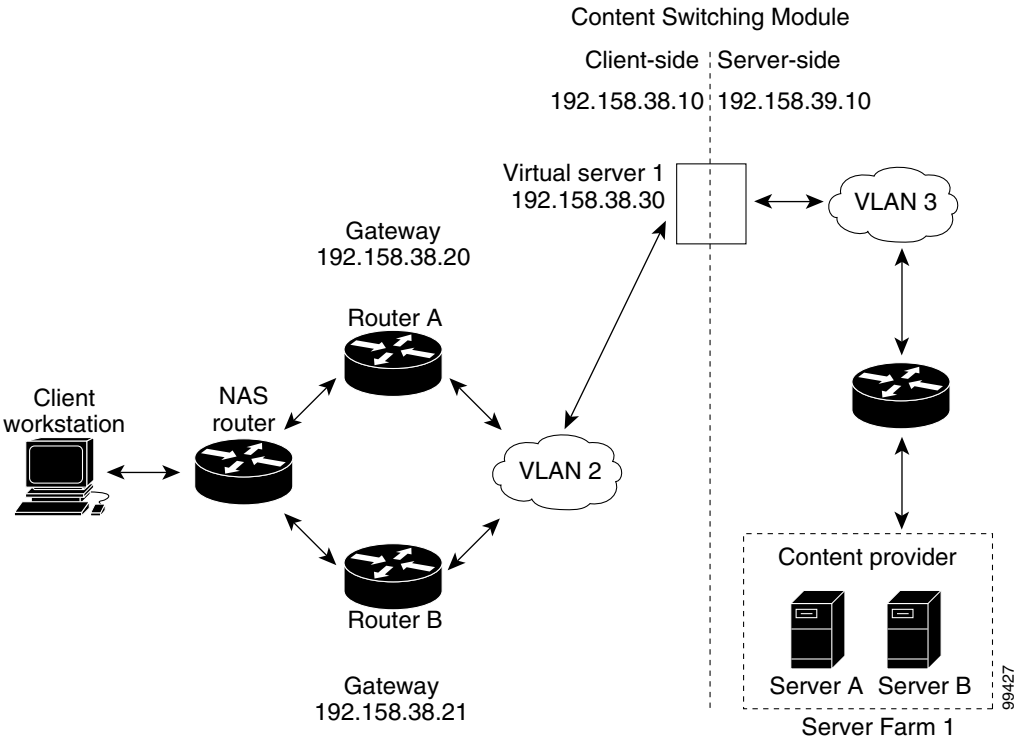
You can set up a fault-tolerant configuration in either the secure (router) or single subnet (bridged) mode using redundant CSMs. For more information, see the "Configuring Fault Tolerance" section on page 7-1.

Single subnet (bridge) mode and secure (router) mode can coexist in the same CSM with multiple VLANs.

Configuring the Secure (Router) Mode

In secure (router) mode, the client-side and server-side VLANs are on different subnets. Figure 2-8 shows how the secure (router) mode configuration is set up.

Figure 2-8 Secure (Router) Mode Configuration



Note The addresses in Figure 2-8 refer to the steps in the following task table.

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

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

	Command	Purpose
Step 9	`Router(config-module-csm)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-server)# ip addr 192.158.39.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-server)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB virtual server mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	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 IP address on the CSM (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 client and server VLANs.

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

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

	Command	Purpose
Step 9	`Router(config-slb-vserver)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-client)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB virtual server mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	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 Router A gateway (192.158.38.20) or the Router B gateway (192.158.38.21).