CHAPTER 1

Overview

The Catalyst 6000 family Content Switching Module (CSM) provides high-performance server load balancing (SLB) between network devices and server farms based on Layer 4 through Layer 7 packet information. Server farms are groups of real servers.

Server farms that are represented as virtual servers can improve scalability and availability of services for your network. You can add new servers and remove failed or existing servers at any time without affecting the virtual server's availability.

Clients connect to the CSM by supplying the virtual IP (VIP) address of the virtual server. When a client initiates a connection to the virtual server, the CSM chooses a real server (a physical device that is assigned to a server farm) for the connection based on configured load-balancing algorithms and policies (access rules). Policies manage traffic by defining where to send client requests for information.

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to *stick* to the same real server using source IP addresses, source IP subnets, cookies, and the secure socket layer (SSL) or by redirecting these connections using the Hypertext Transfer Protocol (HTTP) requests.

Note The CSM runs on Cisco IOS Release 12.1(6)E or later. If you are using a Supervisor Engine 2, you must use Cisco IOS Release 12.1(8a)EX or later. To use the CSM Release 2.1(1), you must be running Cisco IOS Release 12.1(8a)EX or later.
Release 2.2(1) will run with Cisco IOS Release 12.1(8a)EX. However, those features new in CSM Release 2.2(1) will not be available. To use the features added in CSM Release 2.2(1), you must be running Cisco IOS Release 12.1(11b)E or later.

Caution The WS-X6066-SLB-APC Content Switching Module is not fabric enabled.

These sections describe the CSM:

Features

The CSM provides these enhanced features:

- More than one CSM can run in a Catalyst 6000 family switch chassis, and CSMs can run concurrently with Cisco IOS server load balancing (SLB).
- CSM fault-tolerance support allows two CSM modules (in the same or in different chassis) to be configured in the active and standby modes.
- The sticky database and connection table also can be replicated from active to standby to minimize any service disruption.
- CSM firewall load balancing allows you to scale firewall protection.
- A configurable pending-connection timeout feature is available. Pending-connection timeout sets the response time for terminating connections if a switch is flooded with traffic. This feature is used to prevent denial of service (DOS) attacks. Pending connections are configurable on a per virtual server basis.
- The CSM supports 255 VLANs.
- The minimum time between health probes has been reduced to two seconds.

Table 1-1 lists the available CSM features.

Table 1-1 CSM Feature Set Description

Features
Supported Hardware
Supervisor 1A with MSFC and PFC
Supervisor 2
Supported Protocols
TCP load balancing
UDP and all common IP protocol load balancing
Support for FTP and the Real Time Streaming Protocol (RTSP)
Layer 7 Functionality
Full regular expression matching
URL and cookie switching
Generic header parsing
Miscellaneous Functionality
Multiple CSMs in a chassis
CSM and IOS-SLB functioning simultaneously in a chassis
HTTP 1.1 persistence (all GETs to the same server)
Full HTTP 1.1 persistence (GETs balanced to multiple servers)
Fully configurable NAT
Server initiated connections

Table 1-1 CSM Feature Set Description (continued)

Features
Route health injection
Load-balancing Algorithms
Round robin
Weighted round robin
Least connections
Weighted least connections
URL hashing
Source IP hashing
Destination IP hashing
Configurable pending connection timeout
Load Balancing Supported
Server load balancing
Firewall load balancing
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-Ipsec load balancing
Stickiness
Cookie
SSL ID
Source IP
HTTP redirection
Redundancy
Sticky state
Full stateful failover (connection redundancy)
Health Checking
HTTP
ICMP
Telnet
TCP
FTP
SMTP
DNS
Return error code checking

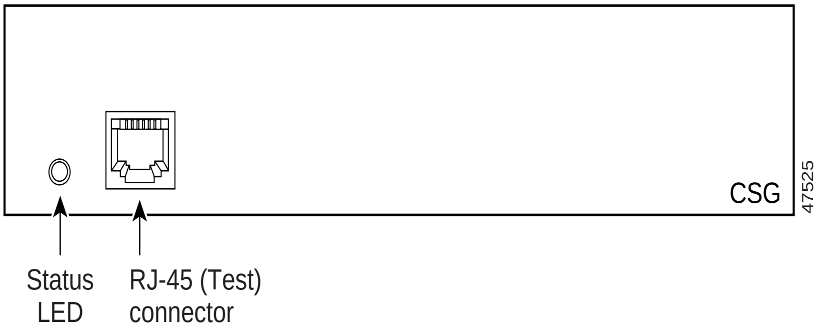
Table 1-1 CSM Feature Set Description (continued)

Features
Inband health checking
Management
SNMP traps

Front Panel Description

Figure 1-1 shows the CSM front panel.

Figure 1-1 Content Switching Module Front Panel



Note The RJ-45 connector is covered by a removable plate.

Status LED

When the CSM powers up, it initializes various hardware components and communicates with the supervisor engine. The Status LED indicates the supervisor engine operations and the initialization results.

Note For more information on the supervisor engine LEDs, refer to the *Catalyst 6000 Family Module Installation Guide*.

During the normal initialization sequence, the status LED changes from off to red, orange, and green. Table 1-2 describes the Status LED operation.

Table 1-2 Content Switching Module Status LED

Color	Description
Off	• The module is waiting for the supervisor engine to provide power. • The module is not on line. • The module is not receiving power, which could be caused by the following: – Power is not available to the CSM. – Module temperature is over the limit[1].
Red	• The module is released from reset by the supervisor engine and is booting. • If the boot code fails to execute, the LED stays red after power up.
Orange	• The module is initializing hardware or communicating with the supervisor engine. • A fault occurred during the initialization sequence. • The module has failed to download its Field Programmable Gate Arrays (FPGAs) on power up, but continues with the remainder of the initialization sequence and provides the module online status from the supervisor engine. • The module has not received module online status from the supervisor engine. This problem could be caused by the supervisor engine detecting a failure in an external loopback test that it issued to the CSM.
Green	• The module is operational; the supervisor engine has provided module online status.
Green to orange	• The module is disabled through the supervisor engine CLI [2] using the **set module disable** *mod* command.

[1] Enter the **show environment temperature** *mod* command to display the temperature of each of four sensors on the CSM.

[2] CLI = command-line interface.

RJ-45 Connector

The RJ-45 connector, which is covered by a removable plate, is used to connect a management station device or a test device. This connector is used by field engineers to perform testing and to obtain dump information.

Operation Mode

Clients and servers communicate through the CSM using Layer 2 and Layer 3 technology in a specific VLAN configuration. (See Figure 1-2.) Clients connect to the client-side VLAN and servers connect to the server-side VLAN. Servers and clients can exist on different subnets. Servers can also be located one or more Layer 3 hops away and connect to the server-side VLAN through routers.

A client sends a request to one of the module’s VIP addresses. The CSM forwards this request to a server that can respond to the request. The server then forwards the response to the CSM, and the CSM forwards the response to the client.

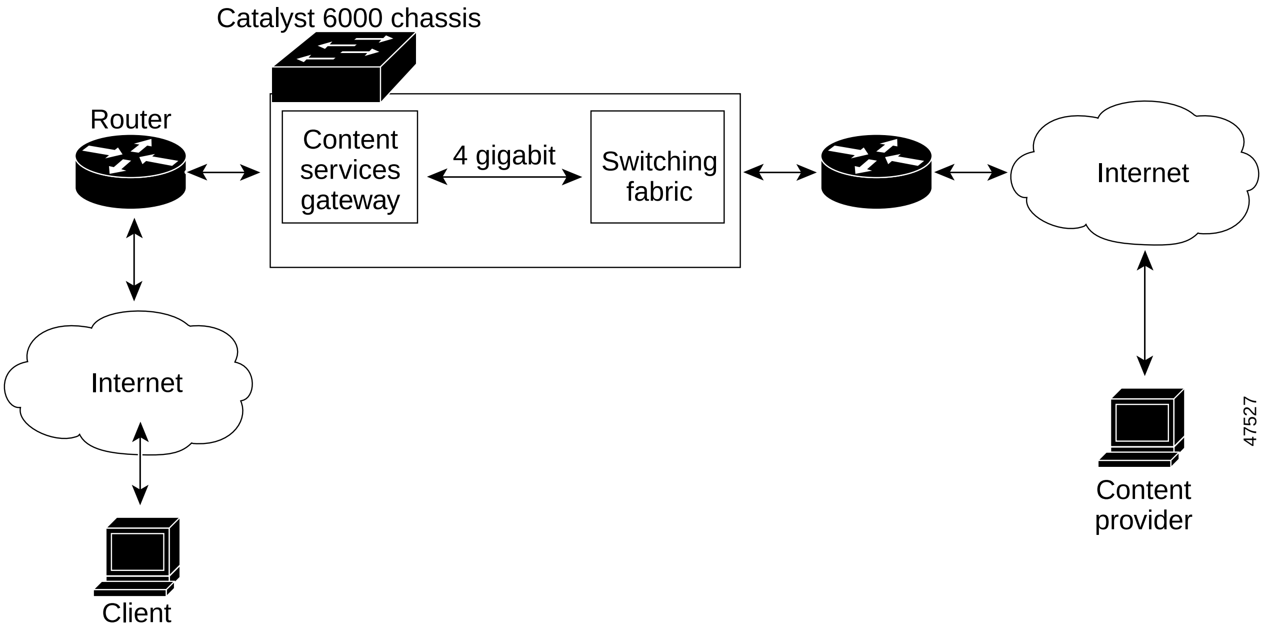
When the client-side and server-side VLANs are on the same subnets, you can configure the CSM in single subnet (bridge) mode. For more information, see the “Configuring the Single Subnet (Bridge) Mode” section on page 4-2.

When the client-side and server-side VLANs are on different subnets, you can configure the CSM to operate in a secure (router) mode. For more information, see the "Configuring the Secure (Router) Mode" section on page 4-4.

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 4-5.

Using multiple VLANs, single subnet (bridge) mode and secure (router) mode can coexist in the same CSM.

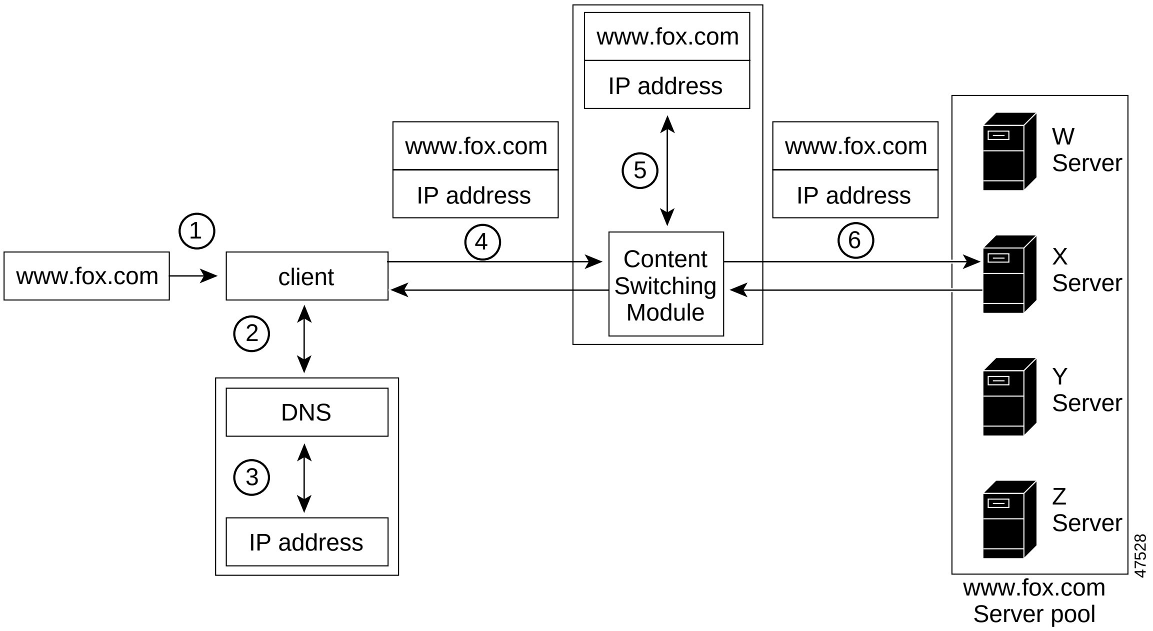
Figure 1-2 Content Switching Module and Servers



Traffic Flow

This section describes how the traffic flows between the client and server in a CSM environment. (See Figure 1-3.)

Figure 1-3 Traffic Flow between Client and Server



Note The numbers in Figure 1-3 correspond to the steps in the following operation procedure.

When you enter a request for information by entering a URL, the traffic flows as follows:

1. You enter a URL. (Figure 1-3 shows www.fox.com as an example.)
2. The client contacts a DNS server to locate the IP address associated with the URL.
3. The DNS server sends the IP address of the virtual IP (VIP) to the client.
4. The client uses the IP address (CSM VIP) to send the HTTP request to the CSM.
5. The CSM receives the request with the URL, makes a load-balancing decision, and selects a server.

   For example, in Figure 1-3, the CSM selects a server (X server) from the www.fox.com server pool, replacing its own VIP address with the address of the X server and forwards the traffic to the X server to allow the servers to initiate connections that do not have matching entries in the NAT configuration. If a NAT server is not specified, the VIP address remains unchanged.
6. The CSM performs Network Address Translation (NAT).