Product Overview

The Catalyst 6500 series Content Switching Module (CSM) provides high-performance server load balancing (SLB) among groups of servers, server farms, firewalls, caches, VPN termination devices, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information.

Server farms are groups of load-balanced devices. 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 directing their requests to 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 connections.

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to *stick* (or attach) 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 Hypertext Transfer Protocol (HTTP) redirect messages.

These sections describe the CSM:

Features

Table 1-1 lists the new CSM features in this release.

Table 1-1 New CSM Feature Set Description

Features New in this Release	Description
Added management features from release 3.1(1)	Includes the XML DTD (document definition type), the Cisco IOS MIB extensions for the CSM, and the system object identifier (SYSOB ID MIB).
Backup (sorry server)	Allows a backup at the real server level.
Denial of service (DoS) improvements	Allows TCP termination for all connections to the CSM providing SYN attacks.
Failover improvements	Provides enhancements for preempt delay, the **forced failover** command, Layer 2 MAC address rewrites, and improved tracking.
Idle and pending timeouts	Allows for the configuration of the idle and pending timeouts for server-initiated connections.
Improved TCL (Toolkit Command Language) functionality	Provides User Datagram Protocol (UDP) socket and global variable support.
Increased VLAN support	Supports up to 512 server and client VLANs.
Jumbo Frame support	Jumbo Frame support has been added to the CSM software release 3.2 to allow support of frames of up to 9 KB for Layer 4 load balancing.
Limited MIB write support	Allow you to change the weights of servers.
Load balancing per packet	Allows the CSM to make load balancing decisions without creating a flow. This feature is useful when load balancing UDP traffic with flows that exist for a short time period, such as DNS.
Route lookup	Allows the CSM to work more efficiently with upstream gateways regardless of their redundancy implementation (HSRP, VRRP, proprietary, etc.)
Stateful Firewall Load Balancing (FWLB)	Allows all connections, both existing and new, to failover to the secondary firewall in a redundant pair. This feature works only with active-active stateful firewall configurations.
Static ARP entry	Provides the ability to manually add entries to the CSM ARP table.
Static sticky entries	The sticky table can be prepopulated with entries to force certain users to connect to specific servers.

Table 1-1 New CSM Feature Set Description (continued)

Features New in this Release	Description
Sticky debug tools	Includes a **show** command for the number of sticky table entries and the ability to enter a specific IP address and receive the sticky information for that IP address.
TCP fragments	Provides support for fragmented TCP packets.
UDP Probe	Provides the ability to send UDP probes to specified ports to verify that the CSM does not receive a "port unreachable" message.
XML configuration from TCL scripts	Adds the ability to send CSM configuration commands within a TCL script.

Table 1-2 lists the CSM features available in this release and previous releases.

Table 1-2 CSM Feature Set Description

Features
Supported Hardware
Supervisor 1A with MSFC and PFC
Supervisor 2 with MSFC and PFC
Supervisor 720—requires CSM software release 3.1(4) or later
Supported Protocols
TCP load balancing
UDP generic IP protocol load balancing
Special application-layer support for FTP and the Real Time Streaming Protocol (RTSP)
Layer 7 Functionality
Full regular expression matching
URL, cookie switching, Generic HTTP header parsing, HTTP method parsing
Miscellaneous Functionality
VIP connection watermarks
Backup (sorry server) and server farm
Optional port for health probes
IP reassembly
TCL (Toolkit Command Language) scripting
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)–requires a license
Resource usage display
Configurable idle and pending connection timeout
Idle timeout for unidirectional flows

Table 1-2 CSM Feature Set Description (continued)

Features
STE integration for SSL load balancing
Real server names
TCP connection redundancy for all types of flows (TCP, UDP, and IP)
Fault tolerant **show** command enhancements
IOS SLB FWLB interoperation (IP reverse-sticky)
Multiple CSMs in a chassis
CSM and IOS-SLB functioning simultaneously in a chassis
Configurable HTTP 1.1 persistence (either all GETs are made to the same server or are balanced to multiple servers)
Fully configurable NAT
Server-initiated connections
Route health injection
Load-balancing Algorithms
Round-robin
Weighted round-robin (WRR)
Least connections
Weighted least connections
URL hashing
Source IP hashing (configurable mask)
Destination IP hashing (configurable mask)
Source and Destination IP hashing (configurable mask)
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-Ipsec load balancing
Generic IP devices and protocols
Stickiness
Cookie sticky with configurable offset and length
SSL ID
Source IP (configurable mask)
HTTP redirection
Redundancy

Table 1-2 CSM Feature Set Description (continued)

Features
Sticky state
Full stateful failover (connection redundancy)
Health Checking
HTTP
ICMP
Telnet
TCP
FTP
SMTP
DNS
Return error-code checking
Inband health checking
User-defined TCL scripts
Management
SNMP traps
Full SNMP and MIB support
XML interface for remote CSM configuration

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. During the normal initialization sequence, the status LED changes from off to red, orange, and green.

Note For more information on the supervisor engine LEDs, refer to the *Catalyst 6500 Series Switch Module Installation Guide*.

Table 1-3 describes the Status LED operation.

Table 1-3 Content Switching Module Status LED

Color	Description
Off	• The module is waiting for the supervisor engine to provide power. • The module is not online. • 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 run, 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

Clients and servers communicate through the CSM using Layer 2 and Layer 3 technology in a specific VLAN configuration. (See Figure 1-2.) In a simple Server Load Balancing (SLB) deployment, 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 CSM 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.

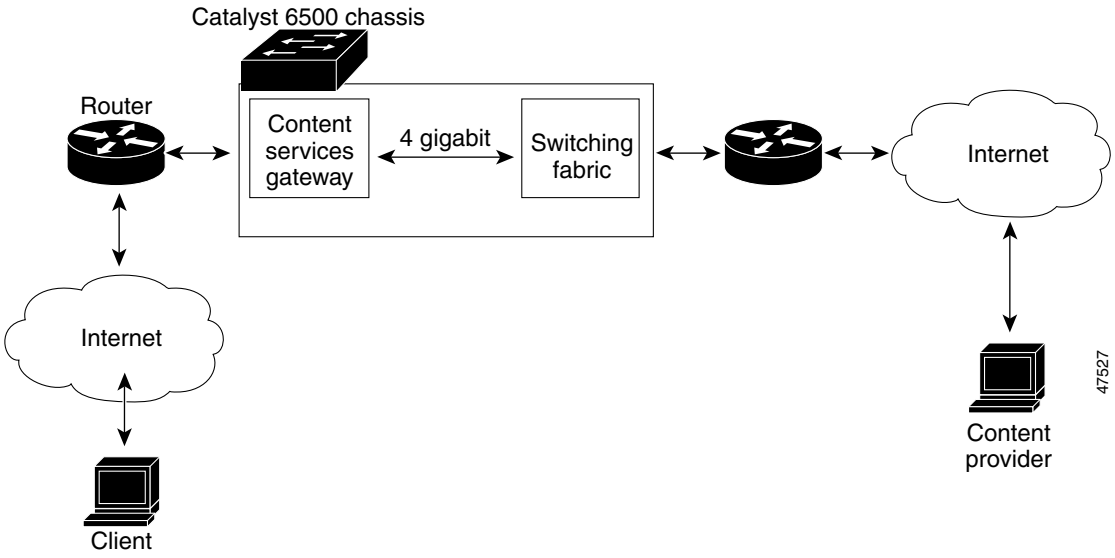
When the client-side and server-side VLANs are on the same subnets, you can configure the CSM in single subnet (bridge) mode. For more information, see the "Configuring the Single Subnet (Bridge) Mode" section on page 2-1.

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 2-4.

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 7-1.

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

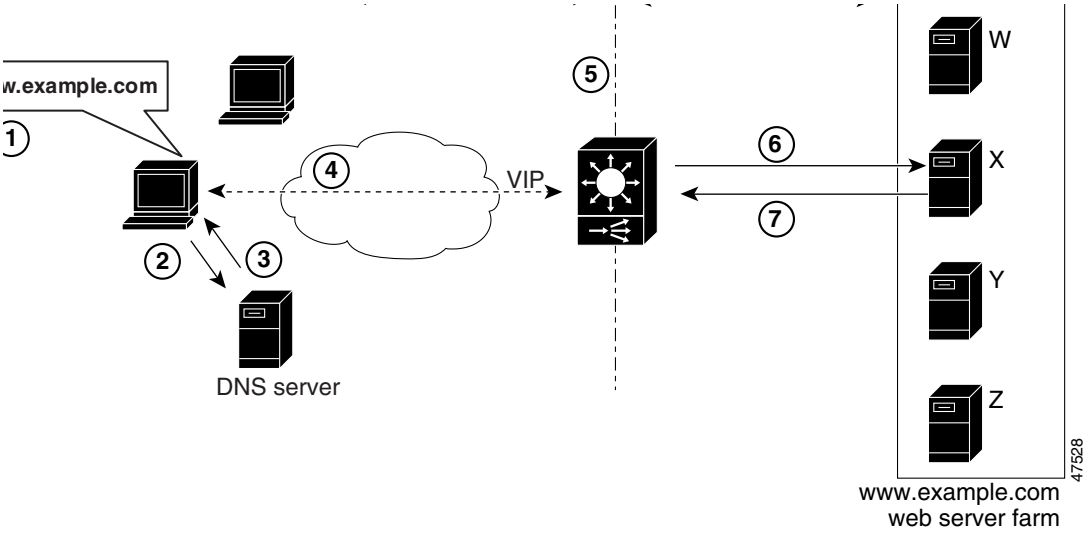
Figure 1-2 Content Switching Module and Servers



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 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.example.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.example.com server pool, replacing its own VIP address with the address of the X server (directed mode), and forwards the traffic to the X server. If the NAT server option is disabled, the VIP address remains unchanged (dispatch mode).
6. The CSM performs Network Address Translation (NAT) and eventually TCP sequence numbers translation.