Overview

The Catalyst 6500 series Content Switching Module (CSM) provides high-performance server load balancing (SLB) among groups of servers, 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* 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.

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 6500 series 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. Multiple firewall farms and DMZs are supported.
- 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 (including the client VLANs, server VLANs and one fault tolerant VLAN used for redundant pairs of CSMs).
- The minimum time between health probes has been reduced to 2 seconds, starting from release 2.1(1).
- Sample scripts are available for reference to support the TCL (Toolkit Command Language) feature. The filename is: c6slb-script.3-1-1a.tcl. This file is located with the CSM Release 3.1(1a) software image at this URL:

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

Table 1-1 New CSM Feature Set Description

New Features New in this Release	Description
VIP connection watermarks	Allow you to limit the number of connections going through a particular virtual server.
Sorry server (backup serverfarm)	Allows you to specify one or more backup servers for use when all primary servers are disabled or out-of-service.
Optional port for health probes	Sets an explicit server port for a probe.
IP reassembly	Attempts reassembly of UDP fragments, even if the first fragment is not received first.
TCL (Toolkit Command Language) scripting	Supports more flexible health probe functionality using administrator-created probe scripts.
XML configuration interface	Allows programmatic configuration of the CSM by a network management device.
SNMP	Does support the CISCO-SLB-MIB and CISCO-SLB-EXT-MIB.
GSLB	Enables global server load balancing.
Resource usage display	Displays resource usage.
Idle timeout for unidirectional flows	Allows uni-directional timeouts for RTSP and other streaming protocols.
SSL termination engine (STE) integration for secure socket layer (SSL) load balancing	Ensures the SSL client is repeatedly connected to the same SSL server, including during SSL ID renegotiation.
HTTP method parsing	Allows HTTP method parsing.

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

New Features New in this Release	Description
Regular expression scalability improvements	Allows more scalable HTTP matching using regular expressions
Real server names	Allows you to name individual real servers. Names can then be used within serverfarms to reference a specific real server.
Non-TCP connection redundancy	Allows non-TCP flows replication to the standby CSM if connection redundancy is configured.
FT show command enhancements	The command displays additional information.
IOS SLB FWLB interoperation (IP reverse-sticky)	Allows you to create reverse sticky entries, allowing firewall load balancing sandwich topologies with IOS SLB.
Slowpath performance improvements	Improves the performance of health probing, configuration changes, and the ability of the CSM to handle ARP traffic. The new XML configuration and TCL scripting features in this release also benefit from this improvement.

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
Supported Protocols
TCP load balancing
UDP and all common 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 and cookie switching
Generic HTTP header parsing
Miscellaneous Functionality
VIP connection watermarks
Sorry server
Optional port for health probes
IP reassembly
TCL (Toolkit Command Language) scripting

Table 1-2 CSM Feature Set Description (continued)

Features
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)
Resource usage display
Idle timeout for unidirectional flows
STE integration for SSL load balancing
HTTP method parsing
Regular expression scalability improvements
Real server names
Non-TCP connection redundancy
FT show command enhancements
IOS SLB FWLB interoperation (IP reverse-sticky)
Slowpath performance improvements
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
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)
Configurable pending connection timeout
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing

Table 1-2 CSM Feature Set Description (continued)

Features
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 (configurable mask)
HTTP redirection
Redundancy
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

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 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 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.

Table 1-3 Content Switching Module Status LED (continued)

Color	Description
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.) In a simple 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.

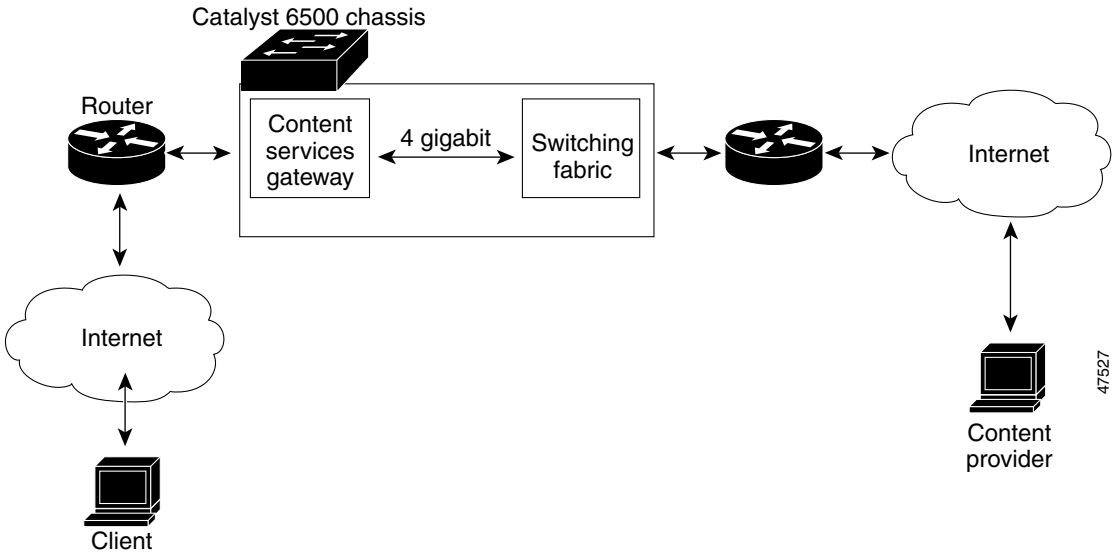
When the client-side and server-side VLANs are on the same subnets, you can configure the CSM in single subnet (bridge) mode. For more information, see the "Configuring the Single Subnet (Bridge) Mode" section on page 4-2.

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.

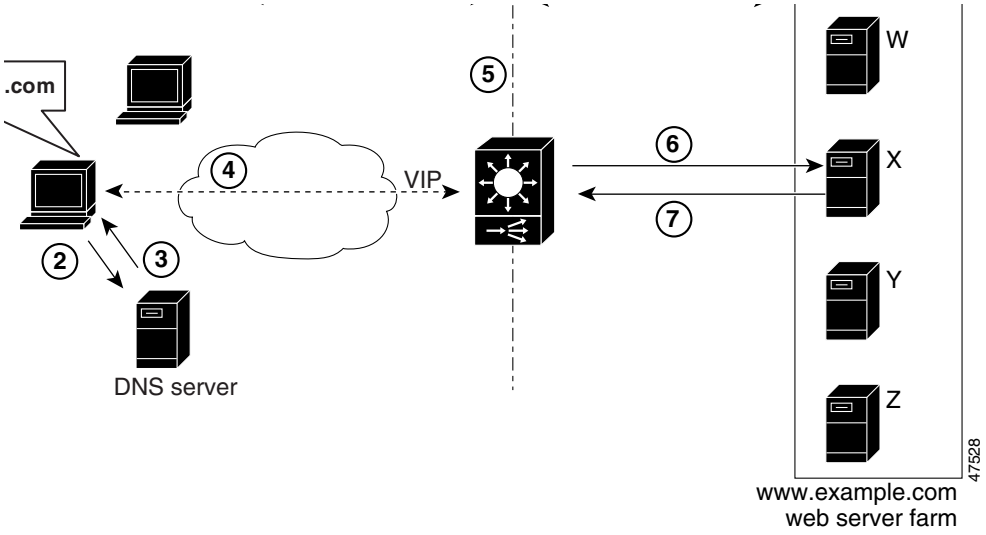
Figure 1-2 Content Switching Module and Servers



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 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.