



Product Overview

This documentation supports these modules:

Product Number: WS-X6066-SLB-S-K9

The Catalyst 6500 Series Content Switching Module with SSL (CSM-S) combines high-performance server load balancing (SLB) with Secure Socket Layer (SSL) offload. The CSM-S can be used to distribute client requests using Layer 3 to Layer 7 information among groups of servers firewalls, caches, VPN termination devices, and other network devices. The CSM-S can also terminate and initiate SSL-encrypted traffic which allows the CSM-S to perform intelligent load balancing while ensuring secure end-to-end encryption.

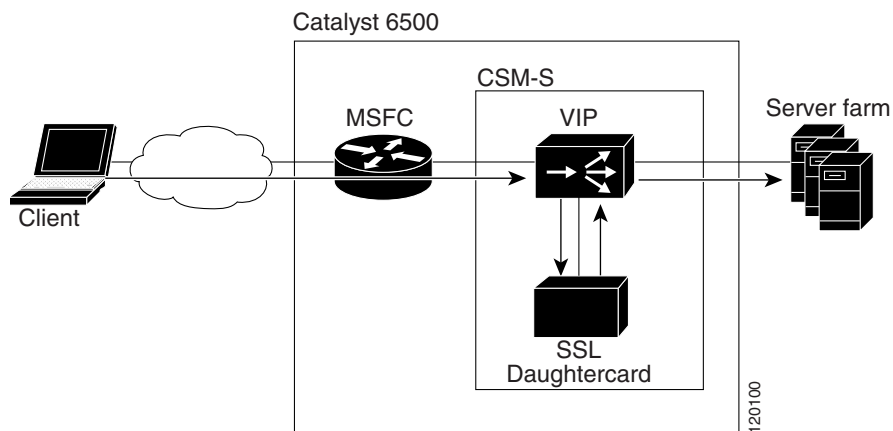


Note

The term *SSL daughter card* refers to the SSL termination daughter card for the CSM-S that accelerates SSL transactions.

Figure 1-1 shows an overview of how traffic flows through the CSM-S between the client and the server farm. 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.

Figure 1-1 CSM-S Traffic Flow Overview



Clients connect to the CSM-S 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-S 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.

When a request arrives encrypted by SSL, the CSM-S can be configured to perform decryption, and eventually apply Layer 7 rules to the clear-text request to select the correct real server. Decryption only occurs if Layer 7 information is required to make the real server selection. If end-to-end encryption is required, the CSM-S re-encrypts the connection request after the real server selection has been made. This process allows the request to continue to the real server in its encrypted form.

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-S:

- [Features, page 1-2](#)
- [Front Panel Description, page 1-8](#)
- [CSM-S and SSL Services Module Command Differences, page 1-10](#)
- [Software Version Information, page 1-10](#)
- [Configuration Restrictions, page 1-12](#)
- [CSM-S Operation Overview, page 1-12](#)
- [CSM-S Operation with SSL, page 1-14](#)

Features

This software release contains feature sets supporting SSL (CSM-S) functionality from previous CSM releases. The tables in this section list these feature sets.

[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
HTTP header sticky	Allows you to configure the CSM to perform stickiness based on the contents of the HTTP header (for example, the mobile station ISDN number [MSISDN], service key, session ID).
Configuration synchronization	Supports the synchronization of the configuration between the active and the standby CSM over the fault tolerant VLAN.
Failover tracking for interfaces and critical devices	Allows you to track the state of HSRP groups, physical interfaces, and gateways.
Private VLANs	Enables the use of private VLANs (PVLANS) with the CSM.

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

Features New in this Release	Description
Partial server farm failover	When you configure a backup server farm, you can define threshold values so that the CSM fails over to the backup server farm if the primary server farm partially fails.
Server probe fail state improvements	Allows you to specify the number of successful retries needed to put a failed server back into service.
Real name option	Allows you to specify details about an entity. This option is applicable for probe, vserver, VLAN, and serverfarm modes
NAT configuration enhancements	Provides source NAT (NAT client) configuration rules to the policy level.
Infinite idle timeout	Allows you to keep a connection open for an indefinite time period.
VIP dependencies	Provides the ability to link VIPs together, providing the ability to automatically take a dependant VIP out of service if the specified VIP goes out of service.
Ordering of policies	Provides the ability to assign a priority value to a particular policy.
Maximum parse length reached behavior change	CSM load balances maximum parse length connection requests to the default policies.
Slow start improvements	Allows real servers to be in slow-start mode until the slow-start timer value expires or the conn_count is equal to that of the other real servers.
Non-secure router mode	Extends the environment variable to route a SYN packet, in addition to a non-SYN packet, that does not hit a VIP.
Increase vserver limit	Increases the number of virtual servers configurable with a particular VIP from 128 to 1000.

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

Table 1-2 CSM Feature Set Description

Features
Supported Hardware
Supervisor 2 with MSFC2
Supported Protocols
TCP load balancing
UDP generic IP protocol load balancing
Special application-layer support for FTP and the Real Time Streaming Protocol (RTSP)
Server Application State Protocol (SASP)
Layer 7 Functionality
Full regular expression matching

Table 1-2 CSM Feature Set Description (continued)

Features
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
SSL Services Module (SSLM) 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

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
Generic IP devices and protocols
Stickiness
Cookie sticky with configurable offset and length
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
XML interface for remote CSM configuration
Back-end encryption support.
Workgroup Manager Support
Server Application State Protocol (SASP)

Table 1-3 lists the CSM-S features in this release.

Table 1-3 CSM-S Feature Set Description

Features
Supported Hardware
Supervisor 2 with MSFC2
Supported Software
Cisco IOS software Release 12.2(18)SXD with the Supervisor Engine 2 and MSFC2
SSL Features
SSL initiation
SSL version 2.0 forwarding
URL rewrite
HTTP header insertion
Wildcard proxy
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Session timeout
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA
Hash Algorithms
MD5
SHA1
Cipher Suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
Public Key Infrastructure
RSA key pair generation for certificates up to 2048 bits
Secure key storage in CSM-S Flash memory device
Certificate enrollment for client and server-type proxy services

Table 1-3 CSM-S Feature Set Description (continued)

Features
Importing and exporting of key and certificate (PKCS12 and PEM)
Duplicating keys and certificates on standby CSM-S using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring keys and certificates
Auto-enrollment and auto-renewal of certificates
Importing of certificate authority certificates by cut-and-paste or TFTP
Up to 8 levels of certificate authority in a certificate chain
Generating of self-signed certificate
Manual certificate enrollment using cut-and-paste or TFTP of PKCS10 CSR file
Peer (client and server) certificate authentication
Peer (client and server) certificates
Certificate security attribute-based access control lists
Certificate revocation lists (CRL)
Certificate expiration warning
TCP Termination
RFC 1323
Connection aging
Connection rate
NAT¹/PAT²
Client and server
Redundancy
When the CSM-S module is in the standby state, you cannot access SSL services.
To have redundancy, you must use either two CSMs or two CSM-S. You cannot mix a CSM and a CSM-S for a supported redundancy configuration.
High Availability
Failure detection (SLB health monitoring schemes)
Module-level redundancy (stateless)
Serviceability
Password recovery
Statistics and Accounting
Total SSL connection attempts per proxy service
Total SSL connections successfully established per proxy service
Total SSL connections failed per proxy service
Total SSL alert errors per proxy service
Total SSL resumed sessions per proxy service

Table 1-3 CSM-S Feature Set Description (continued)

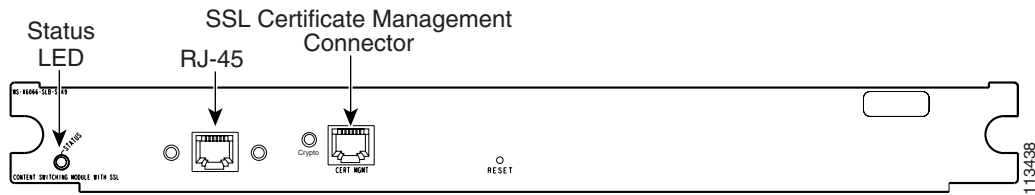
Features
Total encrypted/decrypted packets/bytes per proxy service
Statistics displayed at 1-second, 1-minute, and 5-minute traffic rates for CPU utilization and SSL-specific counters

1. NAT = Network Address Translation
2. PAT = Port Address Translation

Front Panel Description

Figure 1-2 shows the CSM-S front panel.

Figure 1-2 Content Switching Module Front Panel



Note

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

Note

You are required to make initial SSL daughter card configurations through a direct connection to the CSM-S Certificate Management port (Cert. Mgt). After the initial configurations, you can make an SSH or Telnet connection to further configure the module. See the [“Initial SSL Daughter Card Configuration” section on page 5-2](#).

LEDs

When the CSM-S 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, to orange, to green. The SSL daughter card Crypto LED is unused in this release.

Note

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

Table 1-4 describes the Status LED operation.

Table 1-4 Content Switching Module LEDs

LED	Color	Description
Status	Off	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Power is not available to the CSM-S. Module temperature is over the limit¹.
	Red	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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-S.
	Green	<ul style="list-style-type: none"> The module is operational; the supervisor engine has provided module online status.
	Green to orange	<ul style="list-style-type: none"> The module is disabled through the supervisor engine CLI² using the set module disable mod command.
Crypto	None.	<ul style="list-style-type: none"> Not used. Reserved for future releases.

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

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.

SSL Connector

The Certificate Management (Cert. Mgt.) port connector is used for SSL certificate management and is available to make the necessary connection to the SSL daughter card for initial configuration purposes. After the initial configurations, you can make an SSH or Telnet connection to the SSL daughter card to further configure the module. See Chapter 5 in the *Catalyst 6500 Series Content Switching Module with SSL Installation and Configuration Note*.

CSM-S and SSL Services Module Command Differences

This section describes the differences in command functionality between the SSL Services Module and the CSM-S. The following commands or features in the SSL Services Module software are not available in the CSM-S:

- The **debug ssl-proxy pc** command.
- The stateless redundancy feature using HSRP in standalone mode.
- The **virtual ipaddr ...** command under the ssl-proxy service configuration mode requires the **secondary** keyword. The traffic flow will fail if this command is configured without the **secondary** keyword.

For example,

```
'virtual ipaddr 90.1.1.1 protocol tcp port 443' is NOT supported.
'virtual ipaddr 90.1.1.1 protocol tcp port 443 secondary' is supported.
```

- The gateway forward feature from the SSL Services Module does not work with the CSM-S. This feature is used on the SSL Services Module to enable more traffic to flow to the SSL Services Module.

For example,

```
ssl-proxy vlan 2
ipaddr 190.1.1.142 255.255.255.0
gateway 190.1.1.100 forward
```

This feature does not work on the CSM-S because the SSL daughter card receives packets only for the connections that are serviced by a VIP on the CSM. This feature is used on the SSL Services Module to enable more traffic to flow to the SSL Services Module.

Software Version Information

The CSM-S is a combination of the CSM and the SSL Services Module. The version number has these three parts:

A CSM-S version number

A CSM version number

An SSL Services Module version number.

The version number is in the following format:

<CSM-S version> <CSM version> <SSL Services Module version>

For example, the first software release for the CSM-S may appear as follows:

1.1(1) 4.1(3) 2.1(2)



Note

In the following examples, the version numbers are highlighted in **bold** text. There are two **show version** commands available. The **show version** command is available from the supervisor engine CLI and SSL daughter card CLI.

**Note**

The **tech-support processor 0** command displays the CSM software version number.
The **show module** command displays the CSM and SSL bundled software version number.

You can display the version number for the software as follows:

- This example shows how to display the technical support information from the supervisor engine to display the CSM version:

```
Router# show module csm 4 tech-support processor 0
Software version: 4.1(3)
```

- Using the **show module** command from the supervisor engine, for example:

```
Router# show module
Mod Ports Card Type Model Serial No.
-----
 1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-SUP2-2GE SAD055104SU
 2 2 Catalyst 6000 supervisor 2 (Hot) WS-X6K-SUP2-2GE SAL0702BJKF
 3 3 MWAM Module WS-SVC-MWAM-1 SAD071602TZ
 4 3 MWAM Module WS-SVC-MWAM-1 SAD071602UT
 5 3 MWAM Module WS-SVC-MWAM-1 SAD07200176
 7 0 Switching Fabric Module-136 (Active) WS-X6500-SFM2 SAL06355FRR
 8 48 48 port 10/100 mb RJ-45 ethernet WS-X6248-RJ-45 SAD03080474
 9 3 MWAM Module WS-SVC-MWAM-1 SAD0649019F
11 0 CSM with SSL WS-X6066-SLB-S-K9 SAD07380300
12 0 SLB Application Processor Complex WS-X6066-SLB-APC SAD061801NA
13 1 SSL daughter card WS-SVC-SSL-1 SAD070303G2
```

```
Mod MAC addresses Hw Fw Sw Status
-----
 1 0001.6415.ab56 to 0001.6415.ab57 3.2 7.1(1) 12.2(TETONS_ Ok
 2 0006.d65c.5c78 to 0006.d65c.5c79 4.1 7.1(1) 12.2(TETONS_ Ok
 3 0003.feab.9738 to 0003.feab.973f 2.0 7.2(1) 2.1(0.3b) Ok
 4 0002.fcbe.8500 to 0002.fcbe.8507 2.0 7.2(1) 2.1(0.3b) Ok
 5 0003.feab.80c8 to 0003.feab.80cf 2.0 7.2(1) 2.1(0.1b) Ok
 7 0001.0002.0003 to 0001.0002.0003 1.2 6.1(3) 8.3(0.63)TET Ok
 8 0060.09ff.f5c0 to 0060.09ff.f5ef 0.701 4.2(0.24)VAI 8.3(0.63)TET Ok
 9 0005.9a3b.9de8 to 0005.9a3b.9def 0.304 7.2(1) 1.0(0.1) Ok
11 0003.feac.a958 to 0003.feac.a95f 1.7 1.1(1) Ok
12 00d0.d32f.03f8 to 00d0.d32f.03ff 1.5 3.1(6) Ok
13 0040.0bf0.1c04 to 0040.0bf0.1c0b 1.2 7.2(1) 2.1(0.59) Ok
```

- This example shows how to display the SSL proxy version from the SSL daughter card CLI:

```
ssl-proxy> show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SHK(0.28) INTERIM TEST
SOFTWARE
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Tue 04-May-04 11:05 by integ
Image text-base: 0x00400078, data-base: 0x00B04000

ROM: System Bootstrap, Version 12.2(15)YS1 RELEASE SOFTWARE

ssl-proxy uptime is 0 minutes
System returned to ROM by power-on
System image file is "tftp://255.255.255.255/unknown"
AP Version 1.1(1) 4.1(1) 2.1(1)
```

Configuration Restrictions

SSL flows that are processed by the SSL daughter card are flows that are processed only by the CSM. The SSL daughter card cannot off-load flows that are not load balanced by the CSM.

All VLANs that are configured on the SSL daughter card must also be configured on the CSM. If the CSM is not configured, then the traffic for that VLAN will never arrive at the SSL daughter card.

**Note**

There is no configuration verification between the CSM and SSL daughter card. If only the CSM portion of the configuration is completed, the local real servers will show as operational even before the SSL daughter card is configured. The status will always be operational for local real servers. Because these real servers are configured on the daughter card, they are always assumed to be available.

CSM-S Operation Overview

Clients and servers communicate through the CSM-S using Layer 2 and Layer 3 technology in a specific VLAN configuration. (See [Figure 1-3](#).) 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-S through routers.

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

When the client-side and server-side VLANs are on the same subnets, you can configure the CSM-S 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-S to operate in a secure (router) mode. For more information, see the [“Configuring the Secure \(Router\) Mode”](#) section on page 2-3.

You can set up a fault-tolerant configuration in either the secure (router) or single subnet (bridged) mode using redundant CSM-S modules. For more information, see the [“Configuring Fault Tolerance”](#) section on page 9-1.

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

Figure 1-3 Content Switching Module with SSL and Servers

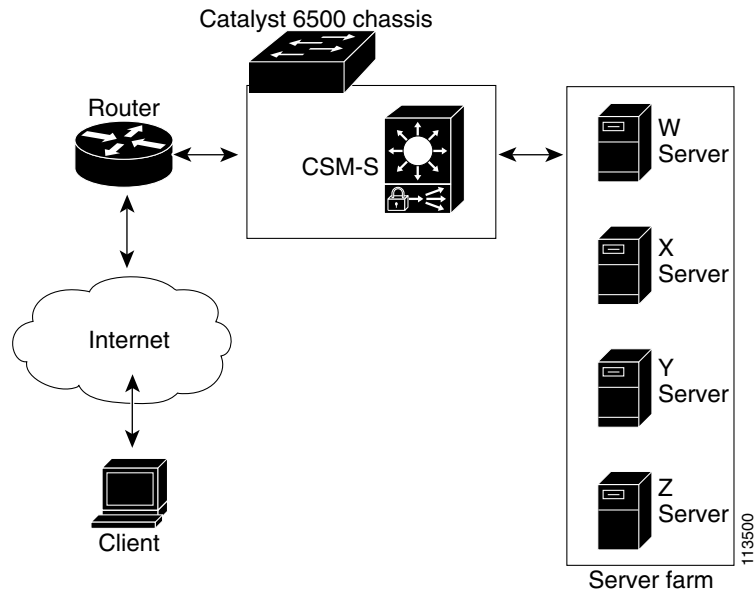
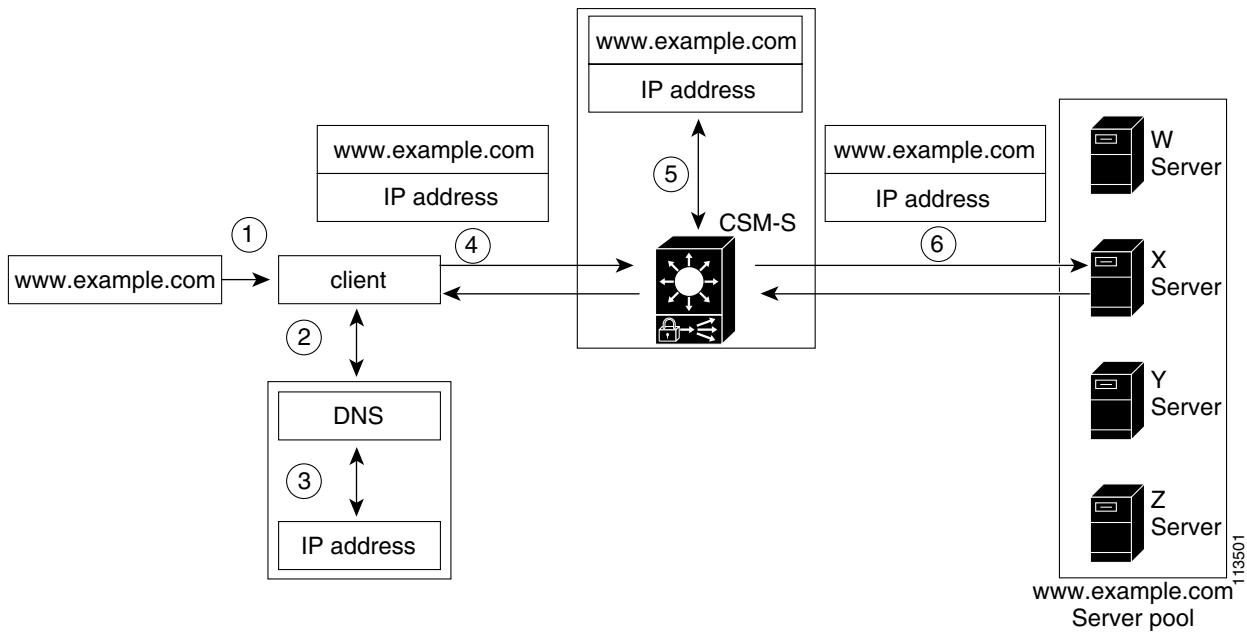


Figure 1-4 describes how the traffic flows between the client and server in a CSM-S environment.

Figure 1-4 Traffic Flow Between Client and Server



Note

The numbers in Figure 1-4 correspond to the numbers in the following operation.

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

1. You enter a URL. (Figure 1-4 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-S VIP) to send the HTTP request to the CSM-S.
5. The CSM receives the request with the URL, makes a load-balancing decision, and selects a server.

For example, in Figure 1-4, the CSM-S 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-S performs Network Address Translation (NAT) and TCP sequence numbers translation.

CSM-S Operation with SSL

The CSM-S is a CSM with integrated SSL support on an internal daughter card so that communication between the load balancing and SSL modules is local to the CSM-S. The CSM-S configuration is a combination of a CSM and SSL Services Module configuration. See Figure 1-5.



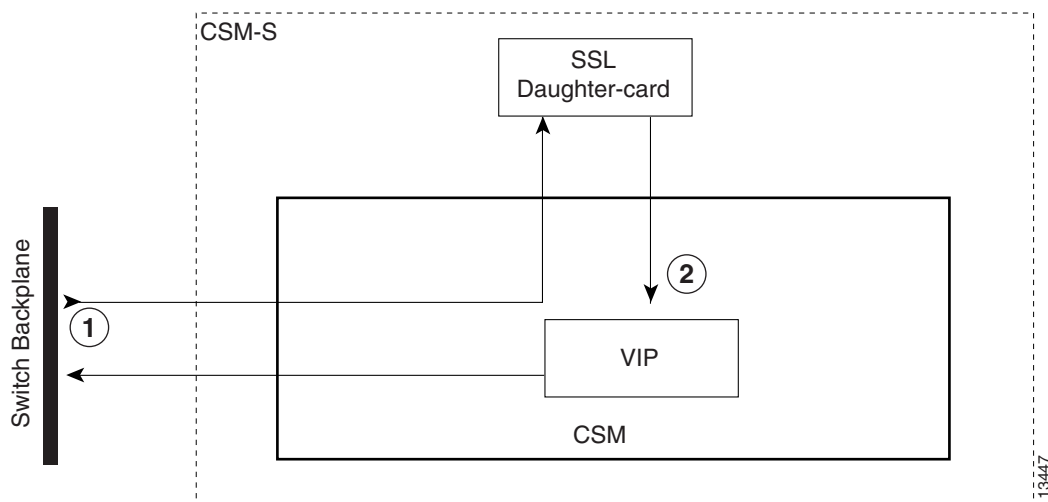
Note

SSL services are available only when virtual servers are configured for SSL operation and VLANs have been configured on the module.

All packets to and from the daughter card are routed through the CSM.

The CSM hardware and the SSL daughter card are loosely coupled but the CSM treats the SSL daughter card as a special real server that it knows is locally attached.

Figure 1-5 CSM-S Hardware Configuration



The daughter card runs the SSL software features from SSL releases up to and including SSL release 2.1 supported by Cisco IOS software Release 12.2(18)SXD. See the “Features” section on page 1-2 for a list of supported features for the CSM-S.

The software runs independently on both the CSM and the SSL daughter card. The CSM-S software allows for SSL configuration and flow processing to and from the daughter card. The Cisco IOS software enables the Public Key Infrastructure (PKI) allowing the CSM-S to load and generate certificates and keys for processing the SSL data flows and to configure the SSL software.

To configure the SSL feature, you must access the daughter card through the Certificate Management (Cert. Mgt.) port. The CSM-S baseboard includes a BOOTP server which upon a daughter card boot request supplies the boot information that includes the IP address and the SSL image to load.

**Note**

When the CSM-S first starts up, the time starts at Jan 1, 1970. Once the CSM and SSL daughter card (CSM-S system) is up, then the time is synchronized with the time on the switch supervisor engine.

You may see syslog messages on the SSL daughter card console referring to expired certificates due to the time synchronization condition on first boot. Once the clock synchronization occurs from the supervisor engine, which occurs within a few seconds after the syslog messages are generated, the CSM-S is ready to pass traffic.

To determine when the CSM-S is ready to pass traffic, you can use the Router# **show module csm slot # status** command.

Two types of syslog messages are displayed when you enter the **show module csm slot # status** command:

1. When the module is ready to pass traffic, this message displays:

```
SLB Module is online in slot 4.  
Configuration Download state: COMPLETE, SUCCESS
```

2. When the module is not ready to pass traffic, this message displays:

```
SLB Module is offline.  
Requires CSM module version 3.1.
```

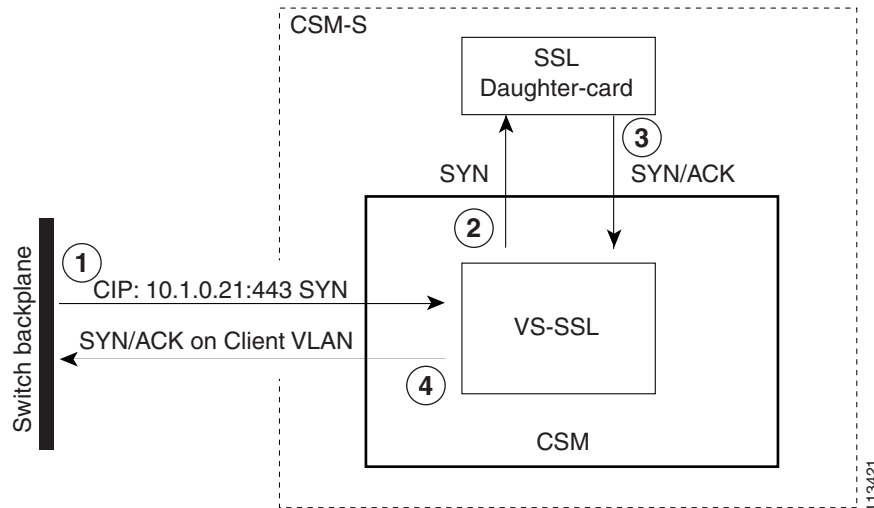
The runtime boot sequence for the CSM-S is as follows:

1. The CSM-S boots.
2. The CSM-S resets the daughter card. The daughter card runs a memory test.
3. When the memory test is complete, the daughter card ROMMON sends a BOOTP request to the CSM-S.
4. The CSM-S sends a BOOTP response containing the MAC address, EOBC IP address, and the flash location from where the daughter card runtime image loads.
5. The SSL console becomes active when the SSL Cisco IOS runtime starts.
6. The SSL software sends a time request to the CSM.
7. The CSM-S indicates to the switch supervisor engine that it is ready to go online.

Client-Side Configuration Traffic Flow

In [Figure 1-6](#), the CSM requires a Layer 4 virtual server configured to accept client traffic on port 443. The server farm associated with this virtual server is configured with the same VIP address as the virtual server and must be marked as being local. Marking the virtual server as local tells the CSM that this server is located on the SSL daughter card. The tables are updated to properly forward traffic to the daughter card.

Figure 1-6 CSM-S Client-Side Configuration

**Note**

The numbers in [Figure 1-6](#) correspond to the numbers in the following operation.

The client-side configuration traffic flow is as follows:

1. When a client SYN-frame is received by the CSM and matches the SSL virtual server, the CSM treats it in the same manner as any Layer 4 virtual server.
2. The destination decision sets up the internal CSM tables to direct all subsequent client traffic on this connection to the SSL daughter card. The reverse tuple is also set up to direct traffic back to the client from the daughter card. The SYN packet is passed to the SSL daughter card for processing.
3. The SSL daughter card processes the SYN-frame and sets up an internal table for connection. The SSL daughter card then responds with a SYN/ACK to the client.
4. The SYN/ACK is received by the CSM and is processed with the reverse tuple. The SYN/ACK is then transmitted to the client through the client VLAN.

This example shows the client-side configuration for the CSM:

```
vlan 420 client
 ip address 192.168.15.109 255.255.255.0
!
serverfarm SSL
 nat server
 no nat client
 real 192.168.15.100 local
 inservice
!
vserver V-SSL
 virtual 192.168.15.200 tcp https
 serverfarm SSL
 persistent rebalance
 inservice
```

This example shows the client-side configuration for the SSL daughter card:

```
ssl-proxy service server_proxy
virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
server ipaddr 192.168.15.200 protocol tcp port 80
certificate rsa general-purpose trustpoint tier1_tp
inservice
ssl-proxy vlan 420
ipaddr 192.168.15.108 255.255.255.0
```

Server-Side Configuration Traffic Flow

When the SSL daughter card terminates the SSL connection, it must establish a connection to a back-end server that services the request. The server is either a real server in the network or a virtual server configured on the CSM.



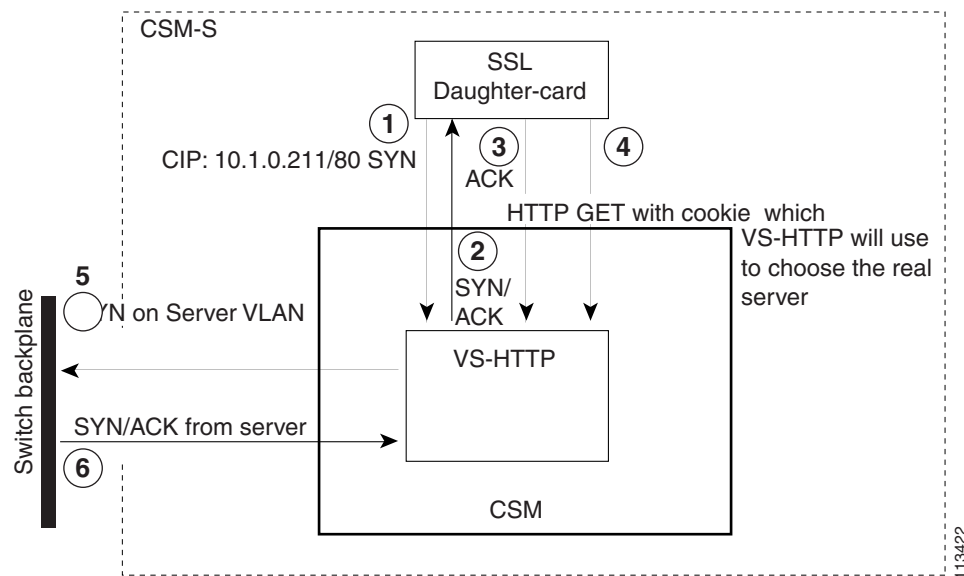
Note

No configuration checking is done between the CSM and the SSL daughter card. You must make sure that the CSM and SSL daughter card configurations are set up correctly to allow the SSL daughter card to use a virtual server on the CSM for Layer 7 load balancing.

Configuring the CSM as the Back-End Server

Figure 1-7 shows the configuration where the back-end server is a Layer 7 virtual server. The virtual server, VS2, is configured to match the ssl-proxy server configuration of the SSL daughter card.

Figure 1-7 CSM-S Server-Side Configuration with CSM as the Back-End Server



Note

The numbers in Figure 1-7 correspond to the numbers in the following operation.

The server-side configuration traffic flow with the CSM as the back-end server is as follows:

1. The SSL daughter card transmits a TCP SYN frame to the target address of the ssl-proxy service.
2. The CSM responds to the SYN that is sent to VS-HTTP with a SYN/ACK to the client IP address, and the SYN/ACK is sent to the SSL daughter card.
3. The SSL daughter card completes the TCP handshake by sending a TCP ACK to the CSM virtual server V-HTTP.
4. The SSL daughter card sends the decrypted HTTP GET request to the CSM virtual server V-HTTP. When the CSM receives this request, it uses the cookie value to determine the actual real server.
5. The CSM sends a TCP SYN to the real server as the client.
6. The real server responds with a TCP SYN/ACK.
7. The CSM continues to operate as it does for Layer 5 and Layer 7 flows for the system.

This example shows the server-side configuration for the CSM:

```
vlan 421 server
 ip address 192.168.17.109 255.255.255.0
!
serverfarm SLB
 nat server
 no nat client
 real 192.168.17.13
 inservice
!
vserver VS-HTTP
 virtual 192.168.15.200 tcp www
 serverfarm SLB
 persistent rebalance
 inservice
```

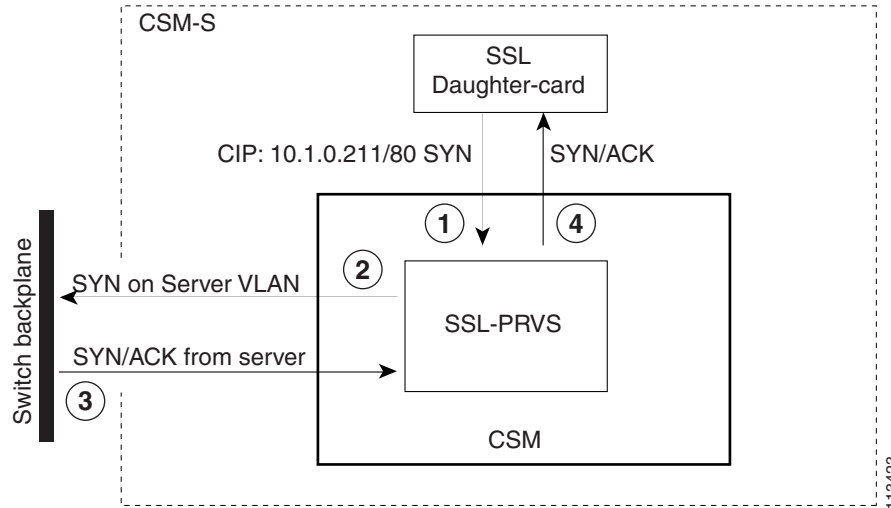
This example shows the server-side configuration for the SSL daughter card:

```
ssl-proxy service server_proxy
 virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
 server ipaddr 192.168.15.200 protocol tcp port 80
 certificate rsa general-purpose trustpoint tier1_tp
 inservice
```

Configuring the Real Server as the Back-End Server

When you configure a real server as the back-end server, the SSL daughter card is configured with the real server's IP address as the SSL-proxy server address. Traffic is sourced by the real server, and the CSM directs traffic from the SSL daughter card to and from the real server.

As shown in [Figure 1-8](#), the CSM is configured with virtual server SSL-PRVS by using a server farm with the predictor-forward option. To properly forward traffic to the real server IP address, the CSM must perform Address Resolution Protocol (ARP) for all possible real servers. For ARP resolution to perform correctly, the server farm SSL real servers must contain the IP address of all possible real servers, but they must not be associated with any virtual server on the CSM. You can also associate health probes with the real servers.

Figure 1-8 CSM-S Server-Side Configuration with a Real Server as the Back-End Server**Note**

The numbers in [Figure 1-8](#) correspond to the numbers in the following operation.

The server-side configuration traffic flow (with the real server as the back-end server) is as follows:

1. The SSL daughter card transmits the TCP SYN frame to the server address of the ssl-proxy service, and that frame is received by the CSM to match the virtual server SSL-PRVS.
2. A load-balancing decision is made, and the frame is forwarded to the server based on the predictor-forward server farm configuration. The reverse tuple is programmed to catch traffic from the server destined to the SSL daughter card. The frame is transmitted on the server VLAN.
3. When the SYN/ACK frame is received on the server VLAN, it matches the reverse path tuple setup and the frame is forwarded back to the client which is the SSL daughter card.
4. The SYN/ACK is sent to the SSL daughter card.

```
vlan 421 server
ip address 192.168.17.109 255.255.255.0
serverfarm SSLPF
  nat server
  no nat client
  predictor forward
vserver SSL-PFVS
  virtual 0.0.0.0 0.0.0.0 tcp 8888
  vlan local
  serverfarm SSLPF
  persistent rebalance
  inservice
```

This example shows the client-side and server-side configuration for the SSL daughter card:

```
ssl-proxy service server_proxy
  virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
  server ipaddr 192.168.17.13 protocol tcp port 8888
  certificate rsa general-purpose trustpoint tier1_tp
  inservice
ssl-proxy vlan 420
  ipaddr 192.168.15.108 255.255.255.0
ssl-proxy vlan 421
  ipaddr 192.168.17.108 255.255.255.0
```

