Getting Started

This chapter describes what is required before you begin configuring the CSM-S and contains these sections:

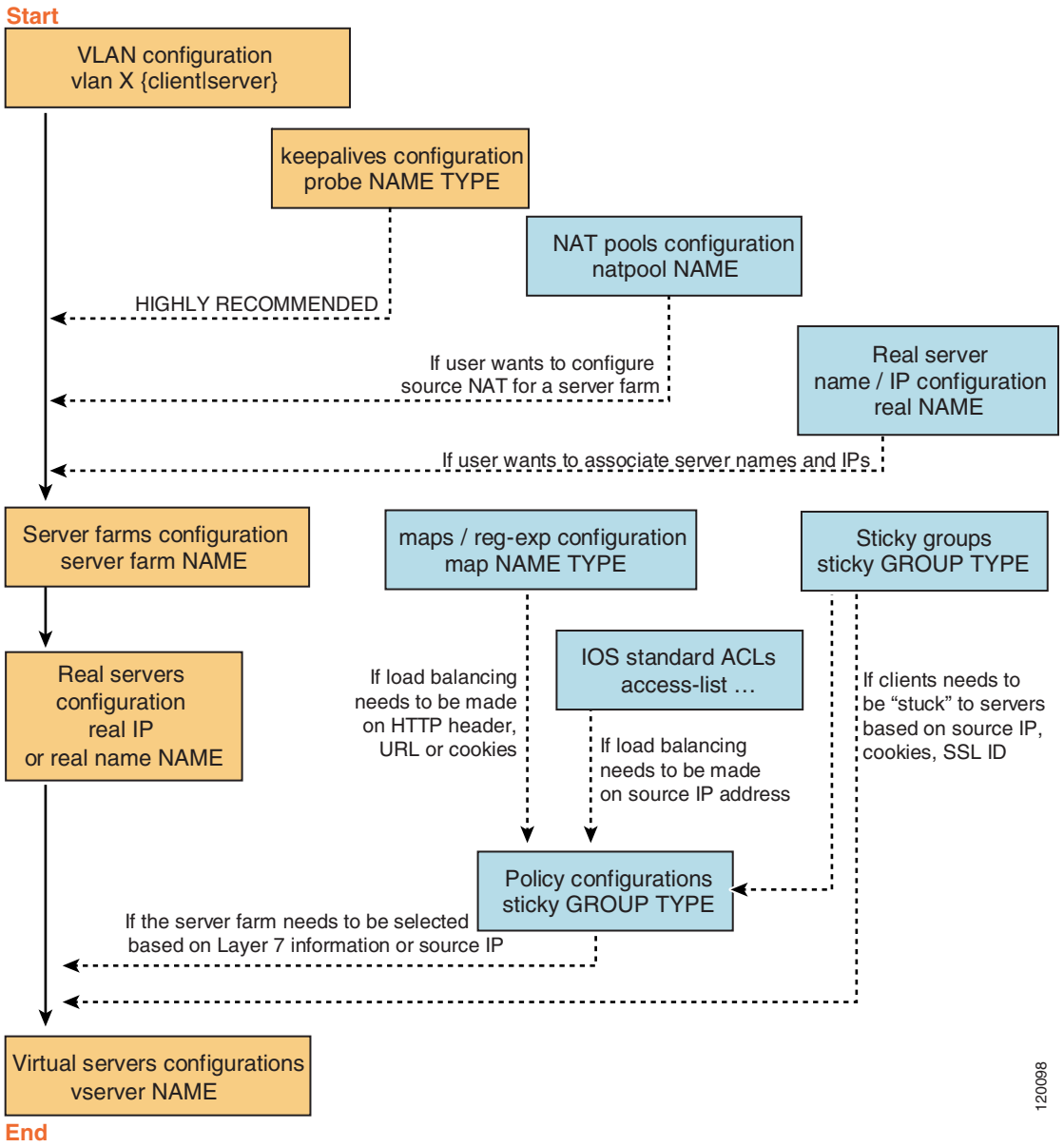
Configuration Overview

The configuration process assumes that the switch is in the RP mode. Figure 3-1 shows an overview of the required and optional operations in the basic CSM-S configuration process. Figure 3-2 shows an overview of the SSL portion of the configuration process.

Note Configuring policies is not necessary for Layer 4 load balancing.

These sections describe how to configure the required parameters:

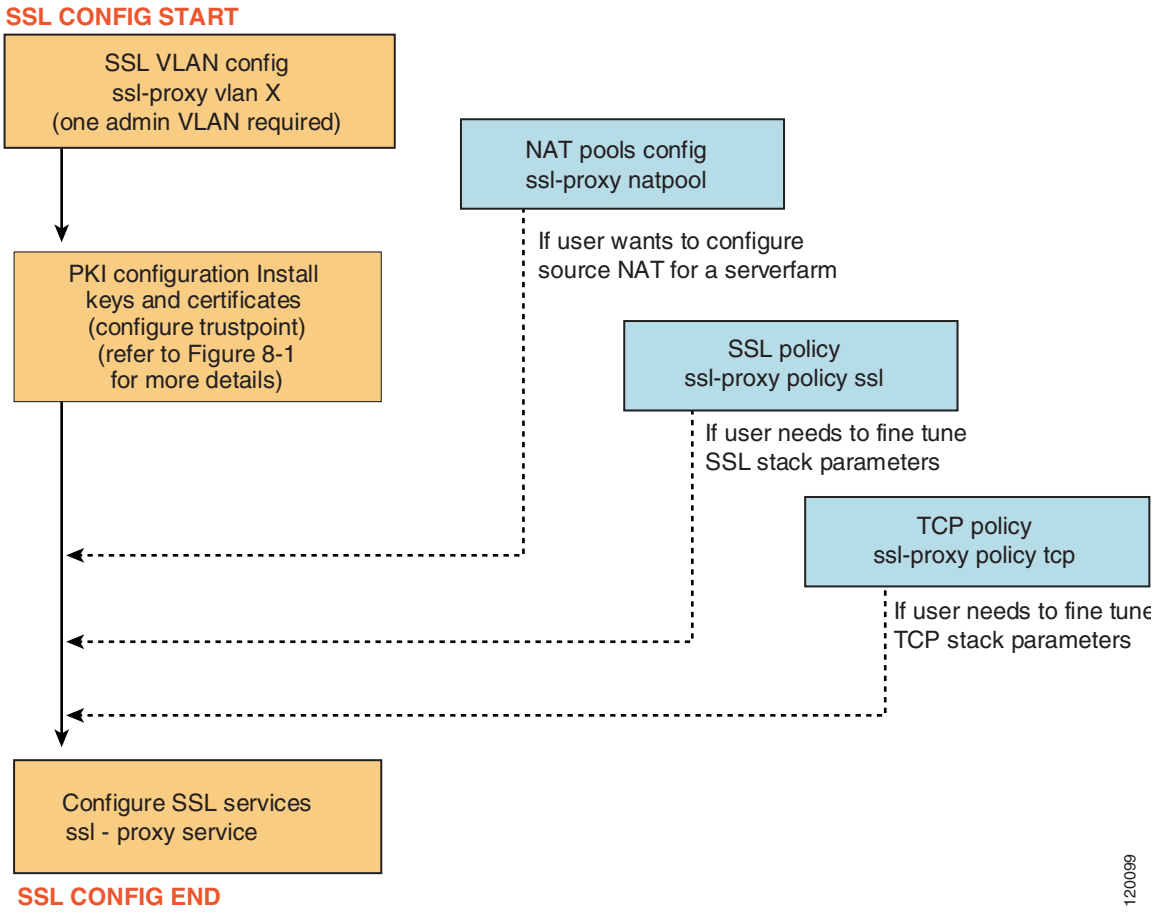
Figure 3-1 CSM-S Basic Configuration Overview



After you configure the required load-balancing parameters on the CSM-S, you can configure the optional parameters in the following sections:

- Configuring Redirect Virtual Servers, page 6-5
- Configuring Client NAT Pools, page 5-6
- Configuring Server-Initiated Connections, page 5-6
- Configuring TCP Parameters, page 6-4

Figure 3-2 CSM-S SSL Configuration Overview



To configure the SSL parameters, see the following sections:

- CSM-S and SSL Services Module Command Differences, page 1-9
- Initial SSL Daughter Card Configuration, page 7-2
- Configuring SSL for Client-Side and Server-Side Operation, page 7-6
- Configuring SSL for Client-Side and Server-Side Operation, page 7-6

To work with advanced configurations, see the following sections in Chapter 2 through Chapter 11:

- Configuring the Single Subnet (Bridge) Mode, page 2-1
- Configuring the Secure (Router) Mode, page 2-3
- Configuring URL Hashing, page 5-7
- Configuring Generic Header Parsing, page 6-10
- Configuring SSL for Client-Side and Server-Side Operation, page 7-6
- Configuring Route Health Injection, page 10-5
- Configuring Fault Tolerance, page 9-1
- Configuring Persistent Connections, page 10-13
- Configuring HSRP, page 9-5

Operating System Support

The CSM-S is supported on switches running only Cisco IOS software. Because the CSM-S is configured through the MSFC CLI, you must first session into the MSFC for access to the MSFC CLI. All the Layer 2 configurations (such as VLAN and port associations) are performed on the supervisor engine when using a switch running the Cisco IOS software.

Note When running the CSM-S on a switch, configured VLANs are automatically added to the trunk or channel that connects the CSM-S to the switch backplane.

Preparing to Configure the CSM-S

Before you configure the CSM-S, you must take these actions:

- Be sure that the Cisco IOS versions for the switch and the module match. Refer to the *Catalyst 6500 Series Switch Content Switching Module Installation Guide*.
- Before you can configure server load balancing, you must obtain the following information:
  - Network topology that you are using in your installation
  - Real server IP addresses
  - An entry for the CSM-S VIPs in the Domain Name Server (DNS) (if you want them to be reached through names)
  - Each virtual server's IP address
- Configure VLANs on the Catalyst 6500 series switch before you configure VLANs for the CSM-S. VLAN IDs must be the same for the switch and the module. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for details.

  This example shows how to configure VLANs:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# vlan 130
Router(config-vlan)# name CLIENT_VLAN
Router(config-vlan)# exit
Router(config)# vlan 150
Router(config-vlan)# name SERVER_VLAN
Router(config-vlan)# end
```

- Place the physical interfaces that connect to the servers or to the clients in the corresponding VLAN.

  This example shows how to configure a physical interface as a Layer 2 interface and assign it to a VLAN:

```
Router>
Router> enable
Router# config
Router(config)# interface 3/1
Router(config-if)# switchport
Router(config-if)# switchport access vlan 150
Router(config-if)# no shutdown
Router(vlan)# exit
```

- If the Multilayer Switch Function Card (MSFC) is used on the next-hop router on either the client or the server-side VLAN, then you must configure the corresponding Layer 3 VLAN interface.

Caution You cannot use the MSFC simultaneously as the router for both the client and the server side unless policy-based routing or source NAT is used and the CSM-S is configured in router mode. This situation occurs because the CSM-S must see both flow directions that load balances or forwards. If you use the CSM-S in bridge (single subnet) mode, do not configure the Layer 3 VLAN interface on the MSFC for both the client and the server side. If you use the CSM-S in router mode, do not configure the Layer 3 VLAN interface on the MSFC for both the client and the server side unless you properly configure policy-based routing or source NAT to direct return traffic back to the CSM-S.

This example shows how to configure the Layer 3 VLAN interface:

```
Router>
Router> enable
Router# config
Router(config)# interface vlan 130
Router(config-if)# ip address 10.10.1.10 255.255.255.0
Router(config-if)# no shutdown
Router(vlan)# exit
```

Using the Command-Line Interface

The software interface for the CSM-S is the Cisco IOS command-line interface. To understand the Cisco IOS command-line interface and Cisco IOS command modes, refer to Chapter 2 in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

Note Because of each prompt's character limit, some prompts may be truncated. For example Router(config-slb-vlan-server)# may appear as Router(config-slb-vlan-serve)#.

Accessing Online Help

In any command mode, you can get a list of available commands by entering a question mark (?) as follows:

```
Router> ?
```

or

```
Router(config)# module CSM 5
Router(config-module-CSM)# ?
```

Note Online help shows the default configuration values and ranges available to commands.

Saving and Restoring Configurations

For information about saving and restoring configurations, refer to the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

Configuring SLB Modes

Server load balancing on the Catalyst 6500 series switch can be configured to operate in two modes: the routed processor (RP) mode and the CSM mode. The switch configuration does not affect CSM-S operation. By default, the CSM-S is configured in RP mode. The RP mode allows you to configure one or multiple CSM-S modules in the same chassis and run Cisco IOS SLB on the same switch.

Note The RP mode is the default mode and is the recommended mode. The CSM mode is used only for backward compatibility with CSM software images previous to release 2.1. When installing a new CSM-S or CSM-S image, use the RP mode.

The CSM mode allows you to configure a single CSM-S only. The CSM mode is supported for backward compatibility with previous software releases. The single CSM-S configuration will not allow Cisco IOS SLB to run on the same switch.

The following sections provide information about the modes:

- Mode Command Syntax, page 3-6
- Migrating Between Modes, page 3-7
- Differences Between the CSM and RP Modes, page 3-8
- Changing Modes, page 3-9

Mode Command Syntax

Before you can enter the CSM-S configuration commands on the switch, you must specify the CSM-S that you want to configure. To specify a CSM-S for configuration, use the **module csm** *slot-number* command. The *slot-number* value is the chassis slot where the CSM-S being configured is located.

The **module csm** command places you in CSM-S configuration submode. All additional configuration commands that you enter apply to the CSM-S that is installed in the slot you have specified.

Note Unless otherwise specified, all the examples in this publication assume that you have already entered this command and entered the configuration submode for the CSM-S that you are configuring.

The command syntax for the CSM-S mode and RP mode configuration is identical with these exceptions:

- When configuring in the CSM mode, you must prefix each top-level command with **ip slb**.
- Prompts are different for the CSM mode and RP mode configurations.

To configure a virtual server for a CSM-S in slot 5, perform this task:

	Command	Purpose
Step 1	`Router(config)# module csm 5`	Specifies the location of the CSM-S that you are configuring.
Step 2	`Router(config-module-csm)# vserver VS1`	Configures the virtual server.

This example shows the complete list of CSM-S commands in the config-module-csm mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# module csm 5
Router(config-module-csm)# ?
SLB CSM module config
  arp          configure a static ARP entry
  capp         configure Content Application Peering Protocol
  default      Set a command to its defaults
  dfp          configure Dynamic Feedback Protocol manager
  exit         exit SLB CSM module submode
  ft           configure CSM fault tolerance (ft) feature
  map          configure an SLB map
  natpool      configure client nat pool
  no           Negate a command or set its defaults
  owner        configure server owner
  policy       configure an SLB policy
  probe        configure an SLB probe
  real         configure module real server
  script       configure script files and tasks
  serverfarm   configure a SLB server farm
  static       configure static NAT for server initiated connections
  sticky       configure a sticky group
  variable     configure an environment variable
  vlan         configure a vlan
  vserver      configure an SLB virtual server
  xml-config   settings for configuration via XML
```

Migrating Between Modes

Existing CSM-S configurations are migrated to the new configuration when the mode is changed from CSM to RP using the **ip slb mode** command. If a CSM-S configuration exists, you are prompted for the slot number.

You can migrate from an RP mode configuration to CSM mode configuration on the Catalyst 6500 series switch. You can migrate manually only from a Cisco IOS SLB configuration to a CSM-S configuration.

Differences Between the CSM and RP Modes

The CSM and RP modes only affect the way in which the CSM-S is configured from the CLI, not the operation and functionalities of the CSM-S itself. The RP mode is required to configure multiple CSM-S modules in one chassis as well as the Cisco IOS SLB in the same chassis with a CSM-S.

CSM Mode

You can use the **ip slb mode csm** command mode to configure a CSM-S in 1.x releases. This mode allows the configuration of a single CSM-S in the chassis (other CSMs or Cisco IOS SLB cannot be configured in the same chassis).

In this mode, all the CSM-S configuration commands begin with **ip slb**.

The CSM-S **show** commands begin with **show ip slb**.

This mode is not recommended if you are using CSM 2.1 or later releases, where it is provided as an option in the Cisco IOS CLI for backward compatibility.

The following is an example of a configuration for a single CSM-S in the chassis:

```
Cat6k# show running-config
Building configuration...
Current configuration : 5617 bytes

ip slb mode csm
ip slb vlan 110 server
ip address 10.10.110.1 255.255.255.0

ip slb vlan 111 client
ip address 10.10.111.2 255.255.255.0
gateway 10.10.111.1

ip slb probe HTTP_TEST http
request method get url /probe/http_probe.html
expect status 200
interval 5
failed 5

ip slb serverfarm WEBFARM
nat server
no nat client
real 10.10.110.10
inservice
real 10.10.110.20
inservice
probe HTTP_TEST

ip slb vserver HTTPVIP
virtual 10.10.111.100 tcp www
persistent rebalance
serverfarm WEBFARM
inservice
```

RP Mode

You can use the **ip slb mode rp** command mode (the default) to configure multiple CSM-S modules in a chassis with Cisco IOS SLB. You can only configure the CSM-S using this mode starting from release 2.1.

In this mode, the CSM-S is configured from this command submode:

mod csm *X*

The *X* is the slot number of the CSM-S that you want to configure.

CSM-S **show** commands start with **show mod csm** *X*.

Beginning with CSM software release 2.1, the RP mode is the recommended mode when configuring the CSM-S. While in this mode, all the commands apply to Cisco IOS SLB and not to a CSM-S in the chassis. These commands begin with **ip slb**.

The following is an example of a configuration for a single CSM-S in the chassis:

```
Cat6k# show running-config
Building configuration...

Current configuration : 5597 bytes
!---

module ContentSwitchingModule 5
vlan 110 server
ip address 10.10.110.1 255.255.255.0

vlan 111 client
ip address 10.10.111.2 255.255.255.0
gateway 10.10.111.1

probe HTTP_TEST http
request method get url /probe/http_probe.html
expect status 200
interval 5
failed 5

serverfarm WEBFARM
nat server
no nat client
real 10.10.110.10
inservice
real 10.10.110.20
inservice
probe HTTP_TEST

vserver HTTPVIP
virtual 10.10.111.100 tcp www
persistent rebalance
serverfarm WEBFARM
inservice
```

Changing Modes

You can change the CSM operating mode from CSM mode to RP mode or RP mode to CSM mode. The next sections provide examples of how to change the modes.

CSM Mode to RP Mode

This example shows how to change from the CSM mode to the RP mode. This example is typical of a migration from CSM 1.x to 2.1 or later releases and does not require a module reset.

```
Cat6k# configure terminal
```

```
 Enter configuration commands, one per line.  End with CNTL/Z.

Cat6k(config)# ip slb mode ?
   csm  SLB in Content Switching Module
   rp   SLB in IOS system

Cat6k(config)# ip slb mode rp
 % The current SLB mode is CSM-SLB.
 % You are selecting RP-SLB mode.
 % All configuration for CSM-SLB will be moved to module submode.
 % Confirm switch to RP-SLB mode? [no]: yes
 % Enter slot number for CSM module configuration, 0 for none [5]: 5
 % Please save the configuration.
Cat6k(config)# end

Cat6k# write
 Building configuration...
 [OK]
Cat6k#
```

RP Mode to CSM Mode

This example shows how to migrate from the RP mode to the CSM mode and requires a module reset:

```
Cat6k# configure terminal
 Enter configuration commands, one per line.  End with CNTL/Z.

Cat6k(config)# ip slb mode ?
   csm  SLB in Content Switching Module
   rp   SLB in IOS system

Cat6k(config)# ip slb mode csm
 % The current SLB mode is RP-SLB.
 % You are selecting CSM-SLB.
 % All SLB configurations for RP will be ERASED.
 % After execution of this command, you must
 % write the configuration to memory and reload.
 % CSM-SLB module configuration will be moved to ip slb submodes.
 % Confirm switch to CSM-SLB mode? [no]: yes
 % Enter slot number for CSM module configuration, 0 for none [5]: 5
 % Please save the configuration and reload.

Cat6k(config)# end
Cat6k# write
 Building configuration...
Cat6k# reload
 Proceed with reload? [confirm] y
Verify Mode Operation
```

Verifying the Configuration

To confirm that your configuration is working properly, use these commands in the RP mode:

```
Cat6k# show ip slb mode
     SLB configured mode = rp

Cat6k# configure terminal
 Enter configuration commands, one per line.  End with CNTL/Z.

Catk6-1(config)# ip slb ?
   dfp           configure Dynamic Feedback Protocol manager
   entries       initial and maximum SLB entries
   firewallfarm  configure an SLB firewall farm
   mode          configure SLB system mode
   natpool       define client nat pool
   probe         configure an SLB probe
   serverfarm    configure an SLB server farm
   vserver       configure an SLB virtual server
```

To confirm that your configuration is working properly, use these commands in the Cisco IOS SLB mode:

```
Cat6k(config)# module csm 5
Cat6k(config-module-csm)# ?
 SLB CSM module config
   default     Set a command to its defaults
   dfp         configure Dynamic Feedback Protocol manager
   exit        exit SLB CSM module submode
   ft          configure CSM fault tolerance (ft) feature
   map         configure an SLB map
   natpool     configure client nat pool
   no          Negate a command or set its defaults
   policy      configure an SLB policy
   probe       configure an SLB probe
   serverfarm  configure an SLB server farm
   static      configure static NAT for server initiated connections
   sticky      configure a sticky group
   vlan        configure a vlan
   vserver     configure an SLB virtual server
```

To confirm that a single CSM-S in the chassis configuration is working properly, use these commands in the CSM mode:

```
Cat6k# show ip slb mode
     SLB configured mode = csm

Catk6-1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Cat6k(config)# ip slb ?
   dfp         configure Dynamic Feedback Protocol manager
   ft          configure CSM fault tolerance (ft) feature
   map         configure an SLB map
   mode        configure SLB system mode
   natpool     configure client nat pool
   policy      configure an SLB policy
   probe       configure an SLB probe
   serverfarm  configure an SLB server farm
   static      configure static NAT for server initiated connections
   sticky      configure a sticky group
   vlan        configure a vlan
   vserver     configure an SLB virtual server
```

Upgrading to a New Software Release

This section describes three methods for upgrading the CSM-S:

- Upgrading from the Supervisor Engine Bootflash, page 3-12
- Upgrading from a PCMCIA Card, page 3-13
- Upgrading from an External TFTP Server, page 3-14

Note When upgrading to a new software release, you must upgrade the CSM-S image before upgrading the Cisco IOS image. Failure to do so causes the supervisor engine not to recognize the CSM-S. In this case, you would have to downgrade the Cisco IOS image, upgrade the CSM-S image, and then upgrade the Cisco IOS image.

Note During the CSM-S upgrade, both the CSM and the SSL daughter card images are upgraded. You cannot use a CSM image on the CSM-S and you cannot use a CSM-S image on a CSM.

To upgrade the CSM-S, you need to session into the CSM-S module being upgraded. During the upgrade, enter all commands on a console connected to the supervisor engine. Enter each configuration command on a separate line. To complete the upgrade, enter the **exit** command to return to the supervisor engine prompt. See the "Configuring SLB Modes" section on page 3-6.

Caution You must enter the **exit** command to terminate sessions with the CSM-S that is being upgraded. If you do not terminate the session and you remove the CSM-S from the Catalyst 6500 series chassis, you cannot enter configuration commands to the CSM-S unless you press **Ctrl** + **^**, enter **x**, and enter the **disconnect** command at the prompt.

Upgrading from the Supervisor Engine Bootflash

Note Refer to the *Catalyst 6500 Series Supervisor Engine Flash PC Card Installation Note* for instructions on loading images into bootflash.

To upgrade the CSM-S from the supervisor engine bootflash, perform these steps:

Step 1 Enable the TFTP server to supply the image from bootflash as follows:

```
Router>
Router> enable
Router# configure terminal
Router(config)# tftp-server sup-bootflash:c6slb-apc.revision-num.bin
Router(config)
```

Step 2 Set up a session between the supervisor engine and the CSM-S:

```
Router# session slot csm-slot-number processor 0
```

Step 3 Load the image from the supervisor engine to the CSM-S:

```
CSM> upgrade 127.0.0.zz c6slb-apc.revision-num.bin
```

The *zz* is 12 if the supervisor engine is installed in chassis slot 1.
The *zz* is 22 if the supervisor engine is installed in chassis slot 2.

Note The supervisor engine only can be installed in chassis slot 1 or slot 2.

Step 4 Close the session to the CSM-S, and return to the Cisco IOS prompt:

```
CSM> exit
```

Step 5 Reboot the CSM-S by power cycling the CSM-S or by entering the following commands on the supervisor engine console:

```
Router(config)# hw-module module csm-slot-number reset
```

Upgrading from a PCMCIA Card

Note Throughout this publication, the term *Flash PC card* is used in place of the term *PCMCIA card*.

To upgrade the CSM-S from a removable Flash PC card inserted in the supervisor engine, perform these steps:

Step 1 Enable the TFTP server to supply the image from the removable Flash PC card:

```
Router>
Router> enable
Router# configure terminal
Router(config)# tftp-server slotx:c6slb-apc.revision-num.bin
```

The *x* value is 0 if the Flash PC card is installed in supervisor engine PCMCIA slot 0.

Step 2 Set up a session between the supervisor engine and the CSM-S:

```
Router# session slot csm-slot-number processor 0
```

Step 3 Load the image from the supervisor engine to the CSM-S:

```
CSM> upgrade slot0: c6slb-apc.revision-num.bin
```

Note The supervisor engine can only be installed in chassis slot 1 or slot 2.

Step 4 Close the session to the CSM-S and return to the Cisco IOS prompt:

```
CSM> exit
```

Step 5 Reboot the CSM-S by power cycling the CSM-S or by entering the following commands on the supervisor engine console:

```
Router# hw-module module csm-slot-number reset
```

Upgrading from an External TFTP Server

To upgrade the CSM-S from an external TFTP server, perform these steps:

Step 1 Create a VLAN on the supervisor engine for the TFTP CSM-S run-time image download.

Note You can use an existing VLAN; however, for a reliable download, you should create a VLAN specifically for the TFTP connection.

Step 2 Configure the interface that is connected to your TFTP server.

Step 3 Add the interface to the VLAN.

Step 4 Enter the CSM-S **vlan** command.

See Chapter 4, "Configuring VLANs" for more information.

Step 5 Add an IP address to the VLAN for the CSM-S.

Step 6 Enter the **show csm** *slot* **vlan detail** command to verify your configuration.

See Chapter 4, "Configuring VLANs" for more information.

Step 7 Verify the CSM-S connectivity to the TFTP server:

```
Router# ping module csm csm-slot-number TFTP-server-IP-address
```

Step 8 Set up a session between the supervisor engine and the CSM-S:

```
Router# session slot csm-slot-number processor 0
```

Step 9 Upgrade the image:

```
CSM> upgrade TFTP-server-IP-address c6slb-apc.rev-number.bin
```

Step 10 Close the session to the CSM-S and return to the Cisco IOS prompt:

```
CSM> exit
```

Step 11 Reboot the CSM-S by power cycling the CSM-S or by entering the following commands on the supervisor engine console:

```
Router# hw-module module csm-slot-number reset
```

Recovering a Lost Password

Recovering a password for SSL on the CSM-S does not require that you load a separate software image on the system. To recover passwords, use the special commands from the Certificate Management (Cert. Mgt.) port on the CSM-S front panel. Due to security concerns, you can only recover the password through this port.

When recovering lost SSL passwords, the following conditions apply:

- You must have a console connection to both the CSM and the SSL daughter card.
- All traffic to and from the SSL daughter card is interrupted because all SSL traffic when the SSL daughter card is rebooted during the password recovery process.

- Use the following prompts when recovering lost passwords:
  - `CSM>` or `VENUS` for the CSM console
  - `ssl-proxy#` for the SSL daughter card.

To recover the SSL daughter card password, perform this task:

	Command	Purpose
Step 1	`CSM>` **`venus`**	Enables the Venus command line interfaces.
Step 2	`VENUS#` **`set_ssl_password_recovery 1`**	Causes the SSL daughter card to reboot into the password recovery mode. In this mode, the SSL daughter card does not require a password to enter the enable mode.
Step 3	`ssl-proxy#` **`enable`**	Enters enable mode on the module.
Step 4	`ssl-proxy#` **`copy nvram:startup-config running-config`**	Copies the startup configuration to the running configuration.
Step 5	`ssl-proxy#` **`configure terminal`**	Enters the configuration mode.
Step 6	`ssl-proxy(config)#` **`enable password`** *`password`*	Enables the password. **Note** The password is the new password that you want to have as your enable password for the SSL daughter card. If you do not want an enable password, you can enter the **no enable password** command instead.
Step 7	`ssl-proxy(config)#` **`line vty`** *`start_line end_line`*	Sets the virtual terminal starting and stopping console line numbers for which you want the enable password reset.
Step 8	`ssl-proxy(config-line)#` **`login`**	Login.
Step 9	`ssl-proxy(config-line)#` **`password`** *`password`*	Enter the new enable password you want to set for the virtual terminal.
Step 10	`ssl-proxy#` **`copy running-config nvram:startup-config`**	Copies the running configuration to the startup configuration.
Step 11	`VENUS#` **`set_ssl_password_recovery 0`**	Causes the SSL daughter card to reboot into the password recovery mode. In this mode, the SSL daughter card does not require a password to enter the enable mode. Once this command is typed, the SSL daughter card will be rebooted. When it completes the rebooting process, the enable password will be the new one that was set in this procedure.
Step 12	`ssl-proxy(config-line)#` **`end`**	Ends the session.

Caution For security reasons, all private keys are unusable after password recovery.

This example shows how to recover a lost password on the SSL daughter card that is inserted in slot 4 from the SSL daughter card Certificate Management (Cert. Mgt.) console port:

```
CSM> venus
VENUS# set_ssl_password_recovery 4
ssl-proxy# enable
ssl-proxy# copy nvram:startup-config running-config
ssl-proxy# configure terminal
```

```
ssl-proxy(config)# enable password cisco
```

Note Enter the **enable password cisco** command to set the password to **cisco**.

```
ssl-proxy(config)# line vty 0 4
ssl-proxy(config-line)# login
ssl-proxy(config-line)# password cisco
ssl-proxy# copy running-config nvram:startup-config
VENUS# set_ssl_password_recovery 0
ssl-proxy(config-line)# end
```

From the SSL daughter card console port, import the keys from the backup image or regenerate the keys.

See the "Configuring the Keys and the Certificates" section on page 8-2 for information on generating keys and importing keys.