Catalyst 6500 Series Switch Content Switching Module with SSL Command Reference

Software Release 2.1(1)
May, 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7029-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Catalyst 6500 Series Switch Content Switching Module with SSL Command Reference

CONTENTS

Preface

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

This guide contains the commands available for use with the Cisco Content Switching Module with SSL (CSM-S). Use this guide with the *Catalyst 6500 Series Switch Content Switching Module with SSL Installation Note* and the *Catalyst 6500 Series Switch Content Switching Module with SSL Installation and Configuration Note*.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches and network managers who perform any of the following tasks:

- Managing network security
- Configuring firewalls
- Managing default and static routes and TCP and UDP services

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Using Content Switching Module Commands	Introduces you to the CSM commands, access modes, and common port and protocol numbers.
Chapter 2	Content Switching Module with SSL Commands	Provides detailed descriptions of all CSM commands in an alphabetical listing.
Chapter 3	Commands Specific to the Content Switching Module with SSL	Provides detailed descriptions of all SSL commands used by the CSMS in an alphabetical listing.
Appendix A	Acronyms	Lists the acronyms used in this command reference.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional. Default responses to system prompts are in square brackets.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or aguments; for example, {**interface** *interface* **type**}.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments in the screen display for which you supply values are in *`italic screen`* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For more detailed installation and configuration information for the Content Switching Module with SSL, refer to the following publications:

- *Release Notes for the Catalyst 6500 Series Switch Content Switching Module with SSL*
- *Catalyst 6500 Series Switch Content Switching Module with SSL Installation Note*
- *Catalyst 6500 Series Switch Content Switching Module with SSL Command Reference*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*

For more detailed installation and configuration information for SSL services, refer to the following publications:

- *Release Notes for Catalyst 6500 Series SSL Services Module Software Release 2.x*
- *Catalyst 6500 Series Switch SSL Services Module Installation and Verification Note*
- *Catalyst 6500 Series Switch SSL Services Module Command Reference*
- *Catalyst 6500 Series Switch SSL Services Module System Messages*

Use this document in conjunction with the CSM documentation available online at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/csm_3_3 /index.htm

Cisco provides CSM technical tips at the following site:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/index.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Using Content Switching Module Commands

This chapter describes how to use the CSM and CSM-S commands and contains the following sections:

- Using the CSM and CSM-S Commands, page 1-1
- Command Modes, page 1-2

Note Except where specifically differentiated, the term “Content Switching Module” and its acronym “CSM” includes both the Content Switching Module and the Content Switching Module with SSL.

The term “Content Switching Module with SSL” and its acronym “CSM-S” are used only where the information presented is specific to the CSMS.

The term SSL daughter card an SSL termination dauthter card for the CSM that accelerates Secure Socket Layer (SSL) transactions.

Using the CSM and CSM-S Commands

This section provides a brief introduction to using commands and where to go for more information on configuring and using your CSM or CSM-S.

You will use these commands for basic tasks:

Command	Task
write memory	Saving the configuration
write terminal	Viewing the configuration
logging buffered debugging	Accumulating system log (syslog) messages
show logging	Viewing system log (syslog) messages
clear logging	Clearing the message buffer

With the command-line interface (CLI), you can do the following tasks:

- Check the syntax before entering a command.

  Enter a command and press the **?** key to view a quick summary, or precede a command with the **help** command (**help aaa**, for example).

- Abbreviate commands.

  You can use the **config t** command to start configuration mode, the **write t** command statement to list the configuration, and the **write m** commmand to write to Flash memory. In most commands, the **show** command can be abbreviated as **sh**. This feature is called command completion.

- Review possible port and protocol numbers at the following Internet Assigned Numbers Authority (IANA) websites:

  http://www.iana.org/assignments/port-numbers
  http://www.iana.org/assignments/protocol-numbers

- Create your configuration in a text editor, and then cut and paste it into the configuration.

  You can paste in a line at a time or the whole configuration. Always check your configuration after pasting large blocks of text to be sure that all of the text was copied.

For information about how to build your CSM and CSM-S configuration, refer to the *Catalyst 6500 Series Content Switching Module Installation and Configuration Note* and *Catalyst 6500 Series Switch Content Switching Module with SSL Installation and Configuration Note*.

CSM and CSM-S technical documentation is located online at the following websites:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/csms

Command Modes

The CSM and CSM-S contain a command set based on Cisco IOS technologies and provides configurable command privilege modes based on the following command modes:

Note When using these modules on a switch running the Catalyst operating system and Cisco IOS, you must session to the Mutilayer Switch Feature Card (MSFC) for the router prompt.

- Unprivileged mode

  The unprivileged mode allows you to view CSM settings. The unprivileged mode prompt appears as follows when you first access the CSM:

  ```
  Router>
  ```

- Privileged mode

  Any unprivileged mode command will work in privileged mode. Use the **enable** command to start the privileged mode from the unprivileged mode as follows:

  ```
  Router> enable
  Password:
  Router
  ```

  The # prompt is displayed.

Use the **exit** or **end** commands to exit privileged mode and return to unprivileged mode as follows:

```
Router# exit

Logoff

Type help or '?' for a list of available commands.
Router>
```

Use the **disable** command to exit privileged mode and return to unprivileged mode as follows:

```
Router# disable
Router>
```

- Configuration mode

  The configuration mode allows you to change the configuration. All privileged, unprivileged, and configuration commands are available in this mode. Use the **configure terminal** command to start the configuration mode as follows:

```
Router# configure terminal
Router(config)#
```

  Use the **exit** or **end** commands to exit configuration mode and return to privileged mode as follows:

```
Router(config)# end
Router#
```

  Use the **disable** command to exit configuration mode and return to unprivileged mode as follows:

```
Router(config)# disable
Router>
```

- Submodes

  When you are in a submode, the prompt changes to:

```
Router(config-submode_name)#
```

Regular Expressions

Regular expressions used in commands are based on the UNIX filename specification. You will use regular expressions in these commands:

- match protocol http cookie (cookie map submode), page -25
- match protocol http header (header map submode), page -30
- match protocol http url (URL map submode), page -34

Expression	Meaning
″*″	Zero or more characters
“?”	Exactly one character—the [Ctrl + V] key combination must be entered
“\”	Escaped character
“|”	Or
Bracketed range (for example, [0–9])	Matching any single character from the range
Leading ^ in a range	Do not match any in the range

Expression	Meaning
“.\a”	Alert (ASCII 7)
“.\b”	Backspace (ASCII 80
“.\f”	Form-feed (ASCII 12)
“.\n”	Newline (ASCII 10)
“.\r”	Carriage return (ASCII 13)
“.\t”	Tab (ASCII 9)
“.\v”	Vertical tab (ASCII 11)
“.\0”	Null (ASCII 0)
“.\\”	Backslash
“.\x##”	Any ASCII character as specified in two-digit hexadecimal notation

CHAPTER 2

Content Switching Module with SSL Commands

This chapter contains an alphabetical listing of the commands necessary to configure the CSM-S. These commands are unique to server load-balancing (SLB) and Layer 3 switching.

arp

To configure a static ARP entry, use the **arp** command. To remove the static ARP entry from the configuration, use the **no** form of this command.

arp *ip_address mac-address* **vlan** *id*

no arp *ip_address*

Syntax Description

ip_address	IP address that you want associate with the ARP entry.
mac-address	MAC address of the host.
vlan *id*	Identifies the VLAN.

Defaults

This command has no default settings.

Command Modes

CSM configuration submode

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure a static ARP entry:

```
Router(config-module-csm)# arp 1.1.1.1 0123.4567.89ab vlan 3
```

capp udp

To enter the Content Application Peering Protocol (CAPP) User Datagram Protocol (UDP) configuration submode, and then enable the CAPP, use the **capp udp** command. To remove the CAPP UDP configuration, use the **no** form of this command.

capp udp

no capp udp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

CSM configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The CSM implements only the agent side of the CAPP, not the content router functionality. This feature provides Global Server Load Balancing (GSLB) when you use the CSM with a Content Services Switch (CSS), which provides the content router function.

When you enter the CAPP UDP submode, the following commands are available:

- **default**—Sets a command to its default.
- **exit**—Saves changes and exits from the subcommand mode; see the “agent (DFP submode)” command section.
- **no**—Negates a command or sets the specified command to its defaults.
- **options**—Sets optional parameters for a specified IP address. see the “options (CAPP UDP submode)” command section.
- **port**—Configures the CAPP port. Range is from 1 to 65535. Default is 5002, see the “port (CAPP UDP submode)” command section.
- **secure**—Enables encryption, see the “secure (CAPP UDP submode)” command section.

Examples

This example shows how to initiate CAPP UDP agent configuration mode and set the CAPP port:

```
Cat6k-2(config-module-csm)# capp udp
Cat6k-2(config-slb-capp-udp)# port 5002
```

Related Commands

port (CAPP UDP submode)

options (CAPP UDP submode)

To assign session options to an IP address, use the **options** command in the CAPP UDP submode. To remove the options for the specified address from the configuration, use the **no** form of this command.

options *ip_address* **encryption MD5** *secret*

no options *ip_address*

Syntax Description

ip_address	IP address that you want associate with this group of options.
encryption MD5	Specifies MD5 authentication.
secret	The string used in encryption and decryption of the MD5 hashing method. Enter an unquoted text string with a maximum of 31 characters.

Defaults

This command has no default settings.

Command Modes

CSM CAPP UDP submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The CSM applies encryption to packets sent to this destination address or when the CSM receives datagrams with a matching source IP address.

You can set the IP address to 0.0.0.0 to apply encryption to all incoming and outbound datagrams that are not specifically configured. The 0.0.0.0 IP address allows you to set a global security configuration that can be applied to an arbitrary number of peers.

Examples

This example shows the application of a specific option set to 10.6.3.21 and a global option set to all other IP addresses. The CSM encrypts datagrams received from 10.6.3.21 and transmitted to 10.6.3.21 with encryption code mySecret. All other datagrams, received or transmitted, are assigned to the default encryption secret anotherSecret.

```
Cat6k-2(config-slb-capp-udp)# options 10.6.3.21 encryption MD5 mySecret
Cat6k-2(config-slb-capp-udp)# options 0.0.0.0 encryption MD5 anotherSecret
```

Related Commands

capp udp

port (CAPP UDP submode)

To set the port number for CAPP UDP connections, use the **port** command in the CAPP UDP submode. To remove the port from the configuration, use the **no** form of this command.

port *port_num*

no port

Syntax Description

port_num	Specifies the UDP port number. Enter a value of 1 to 65535.

Defaults

The **no** form of this command sets the port to 5002.

Command Modes

CSM CAPP UDP submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set the port for CAPP connections:

```
Cat6k-2(config-slb-capp-udp)# 50
```

Related Commands

capp udp

secure (CAPP UDP submode)

To enable or disable the encryption requirement for inbound CAPP datagrams, use the **secure** command in the CAPP UDP submode. This command prevents unauthorized messages from entering the CSM. To remove the encryption requirement from the configuration, use the **no** form of this command.

secure

no secure

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

CSM CAPP UDP submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Use the **capp udp secure** command with the **capp udp options** command to specify which secure messages are accepted. If you use this command without the **capp udp options** command, the CSM drops all incoming data.

Examples

This example shows how to allow only incoming traffic from 10.6.3.21 encrypted with the encryption code mySecret:

```
Cat6k-2(config-slb-capp-udp)# secure
Cat6k-2(config-slb-capp-udp)# options 10.6.3.21 encryption md5 mySecret
```

Related Commands

capp udp

clear module csm

To force the active CSM to become the standby module, use the **clear module csm** command.

clear module csm [*slot* | **all**] **arp-cache** *ip-address* **connections** [**real** | **vserver**] **counters ft active linecard-configuration sticky** [**1-255** | **all**]

Syntax Description

slot	(Optional) Specifies the CSM location in the switch. Range is from 1 to 9.
all	(Optional) Applies to all online CSM modules.
arp-cache *ip-address*	Clears the SLB ARP cache.
connections	Specifies connections.
real	(Optional) Clears SLB connections for the real servers.
vserver	(Optional) Clears SLB connections for a virtual server.
counters	Clears SLB statistics.
ft active	Clears the CSM fault tolerance state to force a failover.
linecard-configuration	Clears the configuration database stored in the SLB linecard
sticky	Specifies sticky.
1-255	(Optional) Clears the designated sticky group; range is from 1 to 255.
all	(Optional) Clears all sticky entries from the sticky database.

Defaults

This command has no default settings.

Command Modes

Privileged

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When a connection is closed, a reset (RST) is sent to both the client and the server. Counters reset all the CSM statistics information, except for the **show mod csm X tech-support** counters, which are reset any time that you run the **show** command. The **linecard-configuration** command forces a soft-reset of the CSM, which erases all existing connections and run-time information. The CSM then reloads its configuration from Cisco IOS. This process takes about 3 seconds.

The **ft active** command is used to force the active CSM to the failover state. Fault tolerance preempt must not be enabled.

dfp

To enter the Dynamic Feedback Protocol (DFP) submode, and then configure DFP, use the **dfp** command. To remove the DFP configuration, use the **no** form of this command.

dfp [**password** *password* [*timeout*]]

no dfp [**password** *password*]

Syntax Description

password	(Optional) Specifies a password for MD5 authentication.
password	(Optional) Password value for MD5 authentication. This password must be the same on all DFP manager devices. The password can contain 1–64 characters. Valid characters are: a–z, A–Z, 0–9, @, #, $.
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted; the range is from 0 to 65535.

Defaults

Timeout value is 180 seconds.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The timeout option allows you to change the password without stopping messages between the DFP agent and its manager.

During a timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After a timeout expires, the agent sends and receives packets with only the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. The extended timeout allows enough time for you to update the password on all agents and servers before the timeout expires. The embedded timeout also prevents mismatches between agents and servers that have the new password and agents and servers that have the old password.

Examples

This example shows how to initiate DFP agent configuration mode, configure DFP, set the password to flounder, and configure a 60-second timeout:

```
Cat6k-2(config-module-csm)# dfp password flounder 60
Cat6k-2(config-slb-dfp)#
```

Related Commands

show module csm dfp

agent (DFP submode)

To configure the DFP agent to which the CSM is going to communicate, use the **agent** command in the SLB DFP submode. To remove the agent configuration, use the **no** form of this command.

agent *ip-address port* [*keepalive-timeout* [*retry-count* [*retry-interval*]]]

no agent *ip-address port*

Syntax Description

ip-address	IP address of the DFP agent.
port	Port number of the DFP agent.
keepalive-timeout	(Optional) Time period in seconds between keepalive messages; the range is from 1 to 65535.
retry-count	(Optional) Number of consecutive connection attempts or invalid DFP reports received before tearing down the connections and marking the agent as failed; the range is from 0 to 65535.
retry-interval	(Optional) Interval between retries; the range is from 1 to 65535.

Defaults

Keepalive timeout is 0 (no keepalive message).

Retry count is 0 seconds (0 seconds allows infinite retries).

Retry interval is 180 seconds.

Command Modes

SLB DFP configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to initiate the DFP agent, configure a 350-second timeout, and configure the number of retries to 270:

```
Cat6k-2(config-slb-dfp)# agent 111.101.90.10 2 350 270
```

Related Commands

dfp
manager (DFP submode)
show module csm dfp

manager (DFP submode)

To set the port where an external DFP can connect to the CSM, use the **manager** command in SLB DFP submode. To remove the manager configuration, use the **no** form of this command.

manager *port*

no manager

Syntax Description

port	Port number.

Defaults

This command has no default settings.

Command Modes

SLB DFP configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command enables the CSM to listen to DFP connections from an external DFP manager.

Examples

This example shows how to set the DFP manager port:

```
Cat6k-2(config-slb-dfp)# manager 4
```

Related Commands

agent (DFP submode)
dfp
show module csm dfp

exit

To log out of the system or to leave a subcommand mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Command mode

Usage Guidelines

To leave a subcommand mode, use the **exit** command. The **exit** command saves any changes before leaving the submode.

Examples

This example shows how to log out of the CSM:

```
Cat6k-2(config-module-csm)# exit
Cat6k-2(config)#
```

ft group

To enter the fault tolerant submode, and then configure fault tolerance on the CSM, use the **ft group** command. To remove the fault-tolerant configuration, use the **no** form of this command.

ft group *group-id* **vlan** *vlan number*

no ft group

Syntax Description

group-id	ID of the fault-tolerant group. Both CSMs must have the same group ID. Range is from 1 to 254.
vlan *vlan number*	Specifies the VLAN over which heartbeat messages are sent by VLAN number. Both CSMs must have the same VLAN ID. The range is from 2 to 4095.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

A fault-tolerant group is comprised of two Catalyst 6500 series switches each containing a CSM configured for fault-tolerant operation. Each fault-tolerant group appears to network devices as a single device. A network may have more than one fault-tolerant group.

When you enter the fault tolerance group submode, the following commands are available:

- **default**—Sets a command to its default.
- **exit**—Saves changes and exits from the subcommand mode; see the “agent (DFP submode)” command section.
- **failover**—Saves changes and exits from the subcommand mode; see the “failover (fault tolerant submode)” command section.
- **heartbeat-time**—Saves changes and exits from the subcommand mode; see the “heartbeat-time (fault tolerant submode)” command section.
- **no**—Negates a command or sets the specified command to its defaults.
- **preempt**—Sets optional parameters for a specified IP address. See the “preempt (fault tolerant submode)” command section.
- **priority**—Configures the CAPP port. Range is from 1 to 65535; default is 5002. See the “priority (fault tolerant submode)” command section.

Examples

This example shows how to configure a fault-tolerant group named 123 on VLAN 5 and set the failover time to 3 seconds:

```
Cat6k-2(config-module-csm)# ft group 123 vlan 5
Cat6k-2(config-slb-ft)# failover 3
```

Related Commands

failover (fault tolerant submode)
heartbeat-time (fault tolerant submode)
preempt (fault tolerant submode)
priority (fault tolerant submode)
show module csm ft

failover (fault tolerant submode)

To set the time for a standby CSM to wait before becoming an active CSM, use the **failover** command in the SLB fault-tolerant configuration submode. To remove the failover configuration, use the **no** form of this command.

failover *failover-time*

no failover

Syntax Description

failover-time	Amount of time the CSM must wait after the last heartbeat message is received before assuming the other CSM is not operating; the range is from 1 to 65535.

Defaults

Failover time is 3 seconds.

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set a failover period of 6 seconds:

```
Cat6k-2(config-slb-ft)# failover 6
```

Related Commands

ft group
show module csm ft

heartbeat-time (fault tolerant submode)

To set the time interval between heartbeat messages that are transmitted by the CSM, use the **heartbeat-time** command in the SLB fault-tolerant configuration submode. To restore the default heartbeat interval, use the **no** form of this command.

heartbeat-time *heartbeat-time*

no heartbeat-time

Syntax Description

heartbeat-time	Time interval between heartbeat transmissions in seconds; the range is from 1 to 65535.

Defaults

Heartbeat time is 1 second.

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set the heartbeat time to 2 seconds:

```
Cat6k-2(config-slb-ft)# heartbeat-time 2
```

Related Commands

ft group
show module csm ft

preempt (fault tolerant submode)

To allow a higher priority CSM to take control of a fault-tolerant group when it comes online, use the **preempt** command in the SLB fault-tolerant configuration submode. To restore the preempt default value, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is that preempt is disabled.

Command Modes

Privileged

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When you enable preempt, the higher priority CSM preempts the other CSM in the fault-tolerant group when the higher priority CSM comes online. When you enable no preempt, the current primary CSM remains the primary CSM when the next CSM comes online.

Note You must set both members of the fault-tolerant CSM pair to preempt for this feature to work.

Examples

This example shows how to set the fault-tolerance mode to preempt:

```
Cat6k-2(config-slb-ft)# preempt
```

Related Commands

ft group
show module csm ft

priority (fault tolerant submode)

To set the priority of the CSM, use the **priority** command in the SLB fault-tolerant configuration submode. To restore the priority default value, use the **no** form of this command.

priority *value* [**alt** *value*]

no priority

Syntax Description

alt	(Optional) Configures the alternate priority value for the standby CSM.
value	(Optional) Priority of a CSM; the range is from 1 to 254.

Defaults

Value is 10.

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 4.2(1)	Adds the **alt** keyword to specify an alternate value that is sent to the standby CSM.

Usage Guidelines

The CSM with the largest priority value is the primary CSM in the fault-tolerant pair when the modules are both operating.

Examples

This example shows how to set the priority value to 12:

```
Cat6k-2(config-slb-ft)# priority 12
```

Related Commands

ft group
preempt (fault tolerant submode)
show module csm ft

track (fault tolerant submode)

To set the fault-tolerant tracking for the gateway, HSRP group, or interface of the CSM, use the **track** command in the SLB fault-tolerant configuration submode.

track {**gateway** *ip_addr* | **group** *group_number* | **interface** {**async** | **ctunnel** | **dialer** | **fastethernet** | **gigabitethernet**} | **mode** {**all** | **any**}}

Syntax Description

gateway *ip_addr*	Configures a gateway or host for tracking.
group *group_number*	Configures an HSRP group for tracking.
interface async | **ctunnel** | **dialer** | **fastethernet** | **gigabitethernet**	Configures an interface for tracking. The interfaces can be asynchronous, tunnel, dialer, fast Ethernet, or Gigabit Ethernet.
mode all | **any**	Configures tracking mode for all devices or any device.

Defaults

The default setting for **mode** is **any**.

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Usage Guidelines

The CSM with the largest priority value is the primary CSM in the fault-tolerant pair when the modules are both operating.

Examples

This example shows how to set tracking mode for all devices:

```
Cat6k-2(config-slb-ft)# track mode all
```

Related Commands

ft group
preempt (fault tolerant submode)
show module csm ft

hw-module csm standby config-sync

To synchronize the configuration between the active CSM and standby CSM, enter the **hw-module csm standby config-sync** command on the active CSM:

hw-module csm *slot* **standby config-sync**

Syntax Description

slot	Specifies the slot of the active CSM.

Defaults

Route processor mode.

Command Modes

Global configuration

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Usage Guidelines

You can synchronize the configurations between the active and standby CSMs in a single chassis or in separate chassis.

Enter this command after you have configured both the active and standby CSMs for synchronization. Enter this command every time you want to synchronize the configuration.

Synchronization happens over the fault-tolerant VLAN. Since traffic over the fault-tolerant VLAN uses broadcast packets, we recommend that you remove all devices from the fault-tolerant VLAN except those that are necessary for communication between the active and standby CSMs.

If you do not enter the **alt** *standby_ip_address* command on the active CSM before you synchronize the configuration, the VLAN IP addresses on the backup CSM will be removed.

Examples

This example shows how to synchronize the configuration between the active and standby CSMs:

```
Router# hw-module csm 5 standby config-sync
%CSM_SLB-6-REDUNDANCY_INFO:Module 5 FT info:Active:Bulk sync started
%CSM_SLB-6-REDUNDANCY_INFO:Module 5 FT info:Active:Manual bulk sync completed
```

Related Commands

ft group
ip address (VLAN submode)
priority (fault tolerant submode)

ip slb mode

To operate as a CSM load-balancing device instead of a Cisco IOS server load balancing (SLB) device, use the **ip slb mode** command to configure the switch. To remove the **mode** configuration, use the **no** form of this command.

ip slb mode {**csm** | **rp**}

no ip slb mode

Syntax Description

csm	Keyword to select the CSM load-balancing mode that allows you to configure a single CSM only and prohibits the use of Cisco IOS SLB on the Catalyst 6500 series switch.
rp	Keyword to select the route processor Cisco IOS SLB mode and enable module CSM commands for configuring multiple CSMs.

Defaults

Route processor mode

Command Modes

Global configuration

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 2.1(1)	This command now enables **module csm** commands for the **rp** mode.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

We recommend that you use the **rp** mode for all configurations. The **rp** mode allows you to configure both the switch and the CSM or other modules without changing modes.

Note You need to reboot the switch to change the mode.

This command allows you to change from the Cisco IOS SLB mode to the CSM load-balancing mode.

Note Specifying the **no ip slb mode** command is the same as specifying the **rp** mode.

Note In **csm** mode, all **ip slb** commands apply to a CSM module; Cisco IOS SLB is not available. In **rp** mode (the default), **ip slb** commands apply to Cisco IOS SLB. The **module csm** commands are available to configure multiple CSMs.

Examples

This example shows how to configure the CSM load-balancing mode:

```
Cat6k-2(config)# ip slb mode csm
```

Related Commands

module csm
show ip slb mode

map cookie

To create a cookie map, and then enter the cookie map configuration submode for specifying cookie match rules, use the **map cookie** command. To remove the cookie maps from the configuration, use the **no** form of this command.

map *cookie-map-name* **cookie**

no map *cookie-map-name*

Syntax Description

cookie-map-name	Cookie map instance; the character string is limited to 15 characters.
cookie	Enters the cookie map submode.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.

Examples

This example shows how to create a cookie map:

```
Cat6k-2(config-module-csm)# map upnready cookie
```

Related Commands

cookie-map (policy submode)
match protocol http cookie (cookie map submode)
show module csm map

match protocol http cookie (cookie map submode)

To add cookies to a cookie map, use the **match protocol http cookie** command in SLB cookie map configuration submode. Multiple match rules can be added to a cookie map. To remove the cookie map name from the cookie map, use the **no** form of this command.

match protocol http cookie *cookie-name* **cookie-value** *cookie-value-expression*

no match protocol http cookie *cookie-name* **cookie-value** *cookie-value-expression*

Syntax Description

cookie-name	Cookie name; the range is from 1 to 63 characters.
cookie-value *cookie-value-expression*	Specifies a cookie value expression; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB cookie map configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Cookie regular expressions (see "Regular Expressions" section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *cookie-name* = *cookie-value-expression*. Cookie expressions allow spaces if they are escaped or quoted. You must match all cookies in the cookie map.

Examples

This example shows how to add cookies to a cookie map:

```
Cat6k-2(config-slb-map-cookie)# match protocol http cookie albert cookie-value 4*
```

Related Commands

cookie-map (policy submode)
map cookie
show module csm map

map dns

To enter the SLB DNS map mode and configure a DNS map, use the **map dns** command. To remove the DNS map from the configuration, use the **no** form of this command.

map *dns-map-name* **dns**

no map *dns-map-name* **dns**

Syntax Description

dns-map-name	Name of an SLB DNS map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Any match of a DNS regular expression in the DNS map results in a successful match. A maximum of 1023 DNS domains can be configured to a map.

Examples

This example shows how to group DNS domains:

```
Cat6k-2(config-module-csm)# map m1 dns
Cat6k-2(config-slb-map-dns)# exit
Cat6k-2(config)
```

Related Commands

match protocol dns domain (DNS map submode)
show module csm map

match protocol dns domain (DNS map submode)

To add a DNS domain to a DNS map, use the **match protocol dns domain** command in the SLB DNS map configuration submode. To remove the DNS domain from the URL map, use the **no** form of this command.

match protocol dns domain *name*

no match protocol dns domain *name*

Syntax Description

name	Names the DNS domain being mapped.

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 4.1(1)	HTTP method parsing support was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to add domains to a DNS map:

```
Cat6k-2(config-slb-map-dns)# match protocol dns domain cisco.com
```

Related Commands

map dns
show module csm map

map header

To create a map group for specifying HTTP headers, and then enter the header map configuration submode, use the **map header** command. To remove the HTTP header group from the configuration, use the **no** form of this command.

map *name* **header**

no map *name*

Syntax Description

name	Map instance; the character string is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to group HTTP headers and associate them with a content switching policy:

```
Cat6k-2(config-module-csm)# map upnready header
Cat6k-2(config-slb-map-header)# match protocol http header Accept header-value *jpeg*
Cat6k-2(config-slb-map-header)# match protocol http header User-Agent header-value *NT*
Cat6k-2(config-slb-map-header)# match protocol http header Host header-value
www.myhome.com
Cat6k-2(config-slb-map-header)# exit
```

Related Commands

header-map (policy submode)
insert protocol http header (header map submode)
match protocol http header (header map submode)
show module csm map

insert protocol http header (header map submode)

To insert header fields and values into an HTTP request, use the **insert protocol http header** command in SLB header map configuration submode. To remove the header insert item from the header map, use the **no** form of this command.

insert protocol http header *name* **header-value** *value*

no insert protocol http header *name*

Syntax Description

name	Literal name of the generic field in the HTTP header. The name is a string with a range from 1 to 63 characters.
header-value *value*	Specifies the literal header value string to insert in the request.

Defaults

This command has no default settings.

Command Modes

SLB header map configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can also use the %is and %id special parameters for header values. The %is value inserts the source IP into the HTTP header, and the %id value inserts the destination IP into the header. You can only specify each special parameter once per header map.

Examples

This example shows how to specify header fields and values to search upon a request:

```
Cat6k-2(config-slb-map-header)# insert protocol http header client header-value %is
```

Related Commands

header-map (policy submode)
map header
show module csm map

match protocol http header (header map submode)

To specify header fields and values for the CSM to search for when receiving a request, use the **match protocol http header** command in SLB header map configuration submode. Multiple match rules can be added to a header map. To remove the header match rule from the header map, use the **no** form of this command.

match protocol http header *field* **header-value** *expression*

no match protocol http header *field*

Syntax Description

field	Literal name of the generic field in the HTTP header. The range is from 1 to 63 characters.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field; the range is from 1 to 127 characters.

Defaults

This command has no default settings.

Command Modes

SLB header map configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

There are predefined fields, for example, Accept-Language, User-Agent, or Host.

Header regular expressions (see “Regular Expressions” section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a header map in the form *header-name* = *expression*. Header expressions allow spaces if they are escaped or quoted. All headers in the header map must be matched.

Examples

This example shows how to specify header fields and values to search upon a request:

```
Cat6k-2(config-slb-map-header)# match protocol http header Host header-value XYZ
```

Related Commands

header-map (policy submode)
insert protocol http header (header map submode)
map header
show module csm map

map retcode

To enable return code checking, and then enter the return code map submode, use the **map retcode** command. To remove the return code checking from the configuration, use the **no** form of this command.

map *name* **retcode**

no map *name*

Syntax Description

name	Return error code map instance; the character string is limited to 15 characters.
retcode	Keyword to enter the return error code map submode.

Defaults

This command has no default settings.

Command Modes

CSM module submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable return error code checking:

```
Cat6k-2(config-module-csm)# map upnready retcode
```

Related Commands

cookie-map (policy submode)
match protocol http cookie (cookie map submode)
show module csm map

match protocol http retcode (return code map submode)

To specify return code thresholds, count and log return codes, and send syslog messages for return code events received from the servers, use the **match protocol http retcode** command in SLB return code map configuration submode. To remove the return code thresholds, use the **no** form of this command.

match protocol http retcode *min max* **action** {**count** | **log** | **remove**} *threshold* [**reset** *seconds*]

no match protocol http retcode *min max*

Syntax Description

min max	Minimum and maximum range of return codes used to perform a count, log, or remove action.
action count	Increments the statistics of the number of occurrences of return codes received.
action log	Specifies where syslog messages are sent when a threshold is reached.
action remove	Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.
threshold	The number of return occurrences before the log or remove action is taken.
reset *seconds*	(Optional) Number of seconds to wait before the processing can resume.

Defaults

This command has no default settings.

Command Modes

SLB return code map configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *threshold* and **reset** values are not configurable for the **count** action. These commands only are available for the **log** and **remove** actions.

Examples

This example shows how to specify return codes values to search for in an HTTP request:

```
Cat6k-2(config-slb-map-retcode)# match protocol http retcode 30 50 action log 400 reset 30
```

Related Commands

map retcode (SLB policy configuration submode)

map url

To enter the SLB URL map mode and configure a URL map, use the **map url** command. To remove the URL map from the configuration, use the **no** form of this command.

map *url-map-name* **url**

no map *url-map-name*

Syntax Description

url-map-name	Name of an SLB URL map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Any match of a URL regular expression in the URL map results in a successful match. A maximum of 1023 URLs can be configured to a map.

Examples

This example shows how to group URLs and associate them with a content switching policy:

```
Cat6k-2(config-module-csm)# map m1 url
Cat6k-2(config-slb-map-url)# match protocol http url /index.html
Cat6k-2(config-slb-map-url)# match protocol http url /stocks/csco/
Cat6k-2(config-slb-map-url)# match protocol http url *gif
Cat6k-2(config-slb-map-url)# match protocol http url /st*
Cat6k-2(config-slb-map-url)# exit
Cat6k-2(config)
```

Related Commands

match protocol http url (URL map submode)
show module csm map
url-map (policy submode)

match protocol http url (URL map submode)

To add a URL regular expression to a URL map, use the **match protocol http url** command in the SLB URL map configuration submode. Multiple match rules can be added to a URL map. To remove the URL regular expression from the URL map, use the **no** form of this command.

match protocol http [**method** *method-expression*] **url** *url-expression*

no match protocol http [**method** *method-expression*] **url** *url-expression*

Syntax Description

method *method-expression*	(Optional) Specifies the method to match.
url-expression	Specifies the regular expression range; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 4.1(1)	HTTP method parsing support was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

URL regular expressions (see “Regular Expressions” section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *urln*. URL expressions do not allow spaces and only one of the URLs in the map must be matched

The method expression can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a string you specify that must be matched exactly (PROTOPLASM).

Examples

This example shows how to add URL expressions to a URL map:

```
Cat6k-2(config-slb-map-url)# match protocol http url html
```

Related Commands

map url
show module csm map
url-map (policy submode)

module csm

To allow the association of load-balancing commands to a specific CSM module, and then enter the CSM module configuration submode for the specified slot, use the **module csm** command. To remove the **module csm** configuration, use the **no** form of this command.

Note The **module ContentSwitching Module** *slot* command is the full syntax; the **module csm** *slot* command is a valid shortcut.

module csm *slot-number*

no module csm *slot-number*

Syntax Description

slot-number	Slot number where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Global configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

If you want to use the multiple module configuration, you must change the **ip slb mode** command to **rp**. An existing CSM configuration is migrated to the new configuration when you change the mode from **csm** to **rp**. The default mode is **rp**, which allows multiple CSM support and allows the Catalyst operating system and Cisco IOS software to run on the same switch.

Migrating from a multiple module configuration to a single module configuration is supported. Migrating the Cisco IOS SLB configuration to the CSM configuration is not supported.

To remove connections to a real server, use the **clear module csm** *X* connnection command.

The CSM had its own ARP cache, which was populated with ARP entries through ARP learning. The addition of the **arp** option allows you to statically configure ARP entries.

Examples

This example shows how to configure a CSM:

```
Cat6k-2(config)# module csm 5
Cat6k-2(config-module-csm)# vserver VS1
```

Related Commands

ip slb mode

natpool (module CSM submode)

To configure source NAT and create a client address pool, use the **natpool** command in module CSM configuration submode. To remove a **natpool** configuration, use the **no** form of this command.

natpool *pool-name start-ip end-ip* [**netmask** *netmask* | **prefix-length** *leading_1_bits*]

no natpool *pool-name*

Syntax Description

pool-name	Name of a client address pool; the character string is from 1 to 15 characters.
start-ip end-ip	Specifies the starting and ending IP address that define the range of addresses in the address pool.
netmask *netmask*	(Optional) Mask for the associated IP subnet.
prefix-length *leading_1_bits*	(Optional) Mask for the associated IP subnet.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

If you want to use client NAT, you must create at least one client address pool.

A maximum of 255 NAT pool addresses are available for any CSM.

Examples

This example shows how to configure a pool of addresses with the name **web-clients**, an IP address range from 128.3.0.1 through 128.3.0.254, and a subnet mask of 255.255.0.0:

```
Cat6k-2(config-module-csm)# natpool web-clients 128.3.0.1 128.3.0.254 netmask 255.255.0.0
```

Related Commands

nat client (serverfarm submode)
show module csm natpool

variable (module CSM submode)

To specify the environmental variables in the configuration, use the **variable** command. To remove a environmental variables from the configuration, use the **no** form of this command.

variable *name value*

no variable *name*

Syntax Description

name	Specifies a name string for the variable.
value	Specifies a value string for the variable.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 4.2(1)	Added MAX_VSERVERS_PER_VIP; increased ROUTE_UNKNOWN_FLOW_PKTS value to 2 for SYN packets.
CSM release 4.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This table lists the environmental values used by the CSM.

Name	Default	Valid Values	Description
ARP_INTERVAL	300	Integer (15 to 31536000)	Time (in seconds) between ARP requests for configured hosts.
ARP_LEARNED_INTERVAL	14400	Integer (60 to 31536000)	Time (in seconds) between ARP requests for learned hosts.
ARP_GRATUITOUS_INTERVAL	15	Integer (10 to 31536000)	Time (in seconds) between gratuitous ARP requests.
ARP_RATE	10	Integer (1 to 60)	Seconds between ARP retries.
ARP_REPLY_FOR_NO_INSERVICE_VIP	0	0	Integer (0 to 1).
ARP_RETRIES	3	Integer (2 to 15)	Count of ARP attempts before flagging a host as down.
ARP_LEARN_MODE	1	Integer (0 to 1)	Indicates whether the CSM learns MAC addresses on responses only (0) or all traffic (1).

Name	Default	Valid Values	Description
ADVERTISE_RHI_FREQ	10	Integer (1 to 65535)	Frequency (in seconds) that the CSM uses to check for RHI updates.
AGGREGATE_BACKUP_SF_STATE_TO_VS	0	Integer (0 to 1)	Specifies whether to include the operational state of a backup server farm into the state of a virtual server.
COOKIE_INSERT_EXPIRATION_DATE	Fri, 1 Jan 2010 01:01:50 GMT	String (2 to 63 chars)	Configures the expiration time and date for the HTTP cookie inserted by the CSM.
DEST_UNREACHABLE_MASK	65535	Integer (0 to 65535)	Bitmask defining which ICMP destination unreachable codes are to be forwarded.
FT_FLOW_REFRESH_INT	60	Integer (1 to 65535)	Interval for the FT slow path flow refresh in seconds.
HTTP_CASE_SENSITIVE_MATCHING	1	Integer (0 to 1)	Specifies whether the URL (cookie, header) matching and sticky are to be case sensitive.
HTTP_URL_COOKIE_DELIMITERS	/?&#+	String (1 to 64 chars)	Configures the list of delimiter characters for cookies in the URL string.
INFINITE_IDLE_TIME_MAXCONNS	1024	0 to 1 - max conns value	Configures the idle time maximum connections.
MAX_PARSE_LEN_MULTIPLIER	1	Integer (1 to 16)	Multiplies the configured max-parse-len by this amount.
MAX_VSERVERS_PER_VIP	10	Integer (7 to 10)	Specifies the maximum number of virual servers that have the same VIP. The values are specified as powers of 2 (for example, 2^7=128, 2^10=1024).
MAX_PARSE_LEN_MULTIPLIER	1	Integer (1 to 16)	Multiplies the configured max-parse-len by this amount.
NAT_CLIENT_HASH_SOURCE_PORT	0	Integer (0 to 1)	Specifies whether to use the source port to select the client NAT IP address.
ROUTE_UNKNOWN_FLOW_PKTS	0	Integer (0 to 2)	Specifies whether to route SYN or non-SYN packets that do not match any existing flows.
NO_RESET_UNIDIRECTIONAL_FLOWS	0	Integer (0 to 1)	Specifies, if set, that unidirectional flows do not be reset when timed out.
SWITCHOVER_RP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine RP switchover occurs.

Name	Default	Valid Values	Description
SWITCHOVER_SP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine SP switchover occurs.
SYN_COOKIE_INTERVAL	3	Integer (1 to 60)	Specifies the interval (in seconds), at which a new syn-cookie key is generated.
SYN_COOKIE_THRESHOLD	5000	Integer (0 to 1048576)	Specifies the threshold (in number of pending sessions) at which syn-cookie is engaged.
TCP_MSS_OPTION	1460	Integer (1 to 65535)	Specifies the maximum segment size (MSS) value sent by CSM for Layer 7 processing.
TCP_WND_SIZE_OPTION	8192	Integer (1 to 65535)	Specifies the window size value sent by CSM for Layer 7 processing.
VSERVER_ICMP_ALWAYS_RESPOND	false	String (1 to 5 chars)	If the response is “true,” the CSM responds to ICMP probes regardless of virtual server state.
XML_CONFIG_AUTH_TYPE	Basic	String (5 to 6 chars)	Specifies the HTTP authentication type for xml-config: Basic or Digest.

Examples

This example shows how to enable the environmental variables configuration:

```
Router(config-module-csm)# variable ARP_RATE 20
```

Related Commands

module csm
show module csm variable

owner

To configure an owner object, use the **owner** command in module CSM configuration submode. To remove an **owner** configuration, use the **no** form of this command.

owner *name*

no owner

Syntax Description

name	Name of the object owner.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 4.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can define more than one virtual server to the same owner, associate multiple servers to an owner, and apply a connection watermark. After the sum of the number of open connections to all virtual servers in a particular owner reaches the VIP connection watermark level for that owner, new connections to any of these virtual servers are rejected by the CSM.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-module-csm)# owner sequel
```

Related Commands

billing-info (owner submode)
contact-info (owner submode)
maxconns (owner submode)

billing-info (owner submode)

To configure billing information for an owner object, use the **billing-info** command in the owner configuration submode. To remove billing information from the configuration, use the **no** form of this command.

billing-info *billing-address-information*

no billing-info

Syntax Description

billing-address-information	Specifies the owner's billing address.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# billing-info 300 cordera avenue
```

Related Commands

contact-info (owner submode)
owner

contact-info (owner submode)

To configure an e-mail address for an owner object, use the **contact-info** command in owner configuration submode. To remove the contact information from the **owner** configuration, use the **no** form of this command.

contact-info *string*

no contact-info

Syntax Description

string	The owner's information.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# contact-info shaggy@angel.net
```

Related Commands

billing-info (owner submode)
owner

maxconns (owner submode)

To configure the maximum number of concurrent connections allowed for an owner object, use the **maxconns** command in owner configuration submode. To remove the maximum connections from the **owner** configuration, use the **no** form of this command.

maxconns *number*

no maxconns

Syntax Description

number	The number of maximum connections to the owner object.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When the maximum number of connections is reached, the connections are reset and the CSM does not accept further connections.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# maxconns 300
```

Related Commands

billing-info (owner submode)
contact-info (owner submode)
owner

policy

To configure policies, associate attributes to a policy, and then enter the policy configuration submode, use the **policy** command. In this submode, you can configure the policy attributes. The policy is associated with a virtual server in virtual server submode. To remove a policy, use the **no** form of this command.

policy *policy-name*

no policy *policy-name*

Syntax Description

policy-name	Name of an SLB policy instance; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Policies establish rules for balancing connections to servers. They can contain URL maps, cookie maps, header maps, client groups, sticky groups, DSCP values, and server farms. The order in which policies are linked to a virtual server determines the precedence of the policy. When two or more policies match a requested URL, the policy with the highest precedence is selected.

Note All policies should be configured with a server farm.

Examples

This example shows how to configure a policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# url-map url_map_1
Cat6k-2(config-slb-policy)# exit
```

Related Commands

show module csm owner
slb-policy policy-name [priority priority_value]

client-group (policy submode)

To associate an access list with a policy, use the **client-group** command in SLB policy configuration submode. To remove an access list from a policy, use the **no** form of this command.

client-group {*1–99* | *std-access-list-name*}

no client-group

Syntax Description

1–99	Standard IP access list number.
std-access-list-name	Standard access list name.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Only client groups that you create with the **ip access-list standard** command can be associated with an SLB policy. You can only associate one client group with a given SLB policy.

Examples

This example shows how to configure a client group:

```
Cat6k-2(config-slb-policy)# client-group 44
Cat6k-2(config-slb-policy)# exit
```

Related Commands

ip access-list standard
policy
show module csm owner

cookie-map (policy submode)

To associate a list of cookies with a policy, use the **cookie-map** command in SLB policy configuration submode. To remove a cookie map, use the **no** form of this command.

cookie-map *cookie-map-name*

no cookie-map

Syntax Description

cookie-map-name	Name of the cookie list associated with a policy.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can associate only one cookie map with a policy. To configure cookie maps, use the **map cookie** command. The cookie map name must match the name specified in the **map cookie** command.

Examples

This example shows how to configure a cookie-based SLB policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# cookie-map cookie-map-1
Cat6k-2(config-slb-policy)# exit
Cat6k-2(config)
```

Related Commands

map cookie
policy
show module csm owner

header-map (policy submode)

To specify the HTTP header criteria to include in a policy, use the **header-map** command in SLB policy configuration submode. To remove a header map, use the **no** form of this command.

Note If any HTTP header information is matched, the policy rule is satisfied.

header-map *name*

no header-map

Syntax Description

name	Name of the previously configured HTTP header expression group.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Only one header map can be associated with a policy. The header map name must match the name specified in the **map header** command.

Examples

This example shows how to configure a header-based policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# header-map header-map-1
Cat6k-2(config-slb-policy)# exit
```

Related Commands

map header
policy
show module csm owner

nat client (policy submode)

To specify a set of client NAT pool addresses that should be used to perform the NAT function on clients connecting to this policy, use the **nat client** command in SLB serverfarm configuration submode. To remove the NAT pool from the configuration, use the **no** form of this command.

nat client {*client-pool-name* | **static**}

no nat client

Syntax Description

client-pool-name	Client pool name.
static	Enables static NAT.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Usage Guidelines

Use this command to enable client NAT. If client NAT is configured, the client address and port number in load-balanced packets are replaced with an IP address and port number from the specified client NAT pool. This client pool name must match the pool name entered from a previous **natpool** command.

If both the serverfarm and the policy are configured with client NAT, the policy takes precedence over the server farm.

Examples

This example shows how to specify NAT on the client:

```
Cat6k-2(config-slb-policy)# nat client whishers
```

Related Commands

natpool (module CSM submode)
script task
show module csm policy

serverfarm (policy submode)

To associate a server farm with a policy, use the **serverfarm** command in the SLB policy configuration submode. To remove the server farm from the policy, use the **no** form of this command.

serverfarm *primary-serverfarm* [**backup** *sorry-serverfarm* [**sticky**] [**threshold** {**inservice** *real_value*}[**sticky**][**outservice** *real_value*]]

no serverfarm

Syntax Description

primary-serverfarm	Character string used to identify the server farm.
backup *sorry-serverfarm*	(Optional) Sets the sorry server farm name to the backup server farm.
sticky	(Optional) Enables stickiness to the backup server.
threshold	(Optional) Configures the server farm health threshold.
inservice *real_value*	(Optional) Specifies the number of active real servers required for the server farm to be activated.
outservice *real_value*	(Optional) Specifies the minimum number of active real servers required to remain as healthy. The outservice *real_value* must be lower than the inservice *real_value.*

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.1(1)	The sorry server (backup server) option was added to this command.
CSM release 4.2(1)	The **threshold inservice** *real_value* and **outservice** *real_value* options were added to this command.

Usage Guidelines

Use the **serverfarm** command to configure the server farm. Only one server farm can be configured per policy. The server farm name must match the name specified in the **serverfarm** module CSM configuration submode command. By default, the sticky option does not apply to the backup server farm. To remove the backup server farm, you can either use the **serverfarm** command without the backup option or use the **no serverfarm** command.

The **backup** *sorry-serverfarm* [**sticky**] value defines whether the sticky group applied to the primary server farm is also applied for the backup server farm. If you do not specify stickiness for the primary server farm, then stickiness also is not applied to the backup server farm.

For example, if you have a sticky group configured for a policy, the primary server farm in this policy becomes sticky. The client will be stuck to the configured real server in the primary server farm. When all of the real servers in the primary server farm fail, new requests from this client are sent to the backup server farm.

When the real server in the primary server farm is operational, the following actions result:

- The existing connections to the backup real server continue to be serviced by the backup real server.
- The new requests from the client are sent to the backup real server if the sticky option is enabled for the backup server farm.
- The new requests return to the primary real server if the sticky option is not used on the backup server farm.

Examples

This example shows how to associate a server farm named central with a policy:

```
Cat6k-2(config-module-csm)# policy policy
Cat6k-2(config-slb-policy)# serverfarm central backup domino sticky
```

Related Commands

policy
serverfarm (virtual server submode)
show module csm owner

set ip dscp (policy submode)

To mark packets that match the policy with a DSCP value, use the **set ip dscp** command in the SLB policy configuration submode. To stop marking packets, use the **no** form of this command.

set ip dscp *dscp-value*

no set ip dscp

Syntax Description

dscp-value	The range is from 0 to 63.

Defaults

The default is that the CSM does not store DSCP values.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to mark packets to match a policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# set ip dscp 22
```

Related Commands

policy
show module csm owner

sticky-group (policy submode)

To associate a sticky group and the sticky group attributes to the policy, use the **sticky-group** command in the SLB policy configuration submode. To remove the sticky group from the policy, use the **no** form of this command.

sticky-group *group-id*

no sticky-group

Syntax Description

group-id	ID of the sticky group to be associated with a policy.

Defaults

The default is 0, which means that no connections are sticky.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *group-id* value must match the ID specified in the **sticky** command; the range is from 1 to 255.

Examples

This example shows how to configure a sticky group:

```
Cat6k-2(config-module-csm)# policy policy1
Cat6k-2(config-slb-policy)# sticky-group 5
```

Related Commands

policy
show module csm owner
show module csm sticky
sticky

url-map (policy submode)

To associate a list of URLs with the policy, use the **url-map** command in SLB policy configuration submode. To remove the URL map from the policy, use the **no** form of this command.

url-map *url-map-name*

no url-map

Syntax Description

url-map-name	Name of the URL list to be associated with a policy.

Defaults

The default is no URL map.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Only one URL map can be associated with a policy. To configure URL maps, use the **map url** command.

Examples

This example shows how to associate a list of URLs with a policy named assembly:

```
Cat6k-2(config-module-csm)# policy policy
Cat6k-2(config-slb-policy)# url-map assembly
```

Related Commands

map url
policy
show module csm owner

probe

To configure a probe and probe type for health monitoring, and then enter the probe configuration submode, use the **probe** command. To remove a probe from the configuration, use the **no** form of this command.

probe *probe-name* {**http** | **icmp** | **telnet** | **tcp** | **ftp** | **smtp** | **dns** | **udp** | **script**}

no probe *probe-name*

Syntax Description

probe-name	Name of the probe; the character string is limited to 15 characters.
http	Creates an HTTP probe with a default configuration.
icmp	Creates an ICMP probe with a default configuration.
telnet	Creates a Telnet probe with a default configuration.
tcp	Creates a TCP probe with a default configuration.
ftp	Creates an FTP probe with a default configuration.
smtp	Creates an SMTP probe with a default configuration.
dns	Creates a DNS probe with a default configuration.
udp	Creates a UPD probe with a default configuration.
script	Creates a script probe with a default configuration.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

A probe can be assigned to a server farm in serverfarm submode. The UDP probe requires ICMP because otherwise the UDP probe will be unable to detect when a server has gone down or has been disconnected. You must associate UDP to the supervisor engine and then configure ICMP.

Because the UDP probe is a raw UDP probe, the CSM uses a single byte in the payload for probe responses. The CSM does not expect any meaningful response from the UDP application. The CSM uses the ICMP unreachable message to determine if the UDP application is not reachable. If there is no ICMP unreachable message in the receive timeout, then the CSM assumes that the probe is operating correctly.

If the IP interface of the real server is down or disconnected, the UDP probe does not know that the UDP application is unreachable. You must configure the ICMP probe in addition to the UDP probe for any server.

The CSM uses the DNS probe as the high-level UDP application. You also can use a TCL script to configure this probe.

When configuring Global Server Load Balancing (GSLB) type probes, the **port** submode command is not used to specify which destination UDP port to query. Use the CSM environment variable GSLB_KALAP_UDP_PORT instead. The default is port 5002.

To specify probe frequency and the number of retries for KAL-AP, ICMP, HTTP, and DNS probes when associated with a GSLB server farm environment, the following variables must be used instead of the probe configuration submode commands:

```
GSLB_KALAP_PROBE_FREQ           10
GSLB_KALAP_PROBE_RETRIES        3
GSLB_ICMP_PROBE_FREQ            10
GSLB_ICMP_PROBE_RETRIES         3
GSLB_HTTP_PROBE_FREQ            10
GSLB_HTTP_PROBE_RETRIES         2
GSLB_DNS_PROBE_FREQ             10
GSLB_DNS_PROBE_RETRIES          3
```

Examples

This example shows how to configure an HTTP probe named TREADER:

```
Cat6k-2(config-module-csm)# probe TREADER http
```

Related Commands

probe
show module csm probe

address (probe submode)

To specify a destination IP address for health monitoring, use the **address** command in SLB probe configuration submode. To remove the address, use the **no** form of this command.

address *ip-address* [**routed**]

no address *ip-address*

Syntax Description

ip-address	Specifies the real server's destination IP address.
routed	(Optional) Specifies that the probe is routed according to the CSM routing table.

Defaults

This command has no default settings.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Multiple addresses can be configured for a DNS probe. For an ICMP probe, you can configure one address. Allows the probes to cross the firewall to check the link to the host on the other side. ICMP is the only probe that supports the address parameter without the **routed** option, which is used for firewall load balancing.

Examples

This example shows how to configure an IP address of the real server:

```
Cat6k-2(config-slb-probe-icmp)# address 101.23.45.36
```

Related Commands

probe
show module csm probe

credentials (probe submode)

To configure basic authentication values for an HTTP probe, use the **credentials** command in the SLB HTTP probe configuration submode. To remove the credentials configuration, use the **no** form of this command.

credentials *username* [*password*]

no credentials

Syntax Description

username	Name that appears in the HTTP header.
password	(Optional) Password that appears in the HTTP header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP probes.

Examples

This example shows how to configure authentication for an HTTP probe:

```
Cat6k-2(config-slb-probe-http)# credentials seamless abercrombie
```

Related Commands

probe
show module csm probe

description (serverfarm submode)

To add a description for the server farm, use the **description** command in the SLB probe configuration submode. To remove the description, use the **no** form of this command.

description *line*

no description

Syntax Description

line	Description text.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Usage Guidelines

Examples

This example shows how to add a description:

```
Cat6k-2(config-slb-probe-http)# description Backup Server Farm
```

Related Commands

expect status (probe submode)

To configure a status code for the probe, use the **expect status** command in the SLB HTTP/FTP/Telnet/SMTP probe configuration submode. To remove the status code from the configuration, use the **no** form of this command.

expect status *min-number* [*max-number*]

no expect status *min-number* [*max-number*]

Syntax Description

min-number	Single status code if the *max-number* value is not specified.
max-number	(Optional) Maximum status code in a range.

Defaults

The default range is 0 to 999 (any response from the server is valid).

Command Modes

SLB HTTP/FTP/Telnet/SMTP probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP, FTP, Telnet, and SMTP probes. You can specify multiple status code ranges with this command by entering one command at a time. If you specify the *max-number* value, this number is used as the minimum status code of a range. If you specify no maximum number, this command uses a single number (*min-number*). If you specify both *min-number* and *max-number* values, this command uses the range between the numbers.

Both the minimum number and the maximum number can be any number between 0 and 999 as long as the maximum number is not lower than the minimum number.

For example:

`expect status 5` is the same as **`expect status 5 5`**

`expect status 0` specifies a range of 0 to 4

`expect status 900 999` specifies a range of 900 to 999.

You can specify many expected status ranges.

Note When you remove the expect status, you cannot set the range of numbers to 0 or as a range of numbers that includes the values you set for the expect status. The expect status state becomes invalid and does not restore the default range of 0 through 999. To remove the expect status, remove each set of numbers using the **no expect status** command. For example, enter the **no expect status 0 3** command and then enter the **no expect status 34 99** command.

Examples

This example shows how to configure an HTTP probe with multiple status code ranges:

```
Cat6k-2(config-slb-probe-http)# expect status 34 99
Cat6k-2(config-slb-probe-http)# expect status 0 33
Cat6k-2(config-slb-probe-http)#
```

Related Commands

probe
show module csm probe

failed (probe submode)

To set the time to wait before probing a failed server, use the **failed** command in the SLB probe configuration submode. To reset the time to wait before probing a failed server to default, use the **no** form of this command.

failed *failed-interval*

no failed

Syntax Description

failed-interval	Specifies the interval in seconds before the probe retires a failed server; the range is from 2 to 65535.

Defaults

The default value for the failed interval is 300 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a failed server probe for 200 seconds:

```
Cat6k-2(config-slb-probe-http)# failed 200
```

Related Commands

probe
show module csm probe

header (probe submode)

To configure a header field for the HTTP probe, use the **header** command in the SLB HTTP probe configuration submode. To remove the header field configuration, use the **no** form of this command.

header *field-name* [*field-value*]

no header *field-name*

Syntax Description

field-name	Name for the header being defined.
field-value	(Optional) Content for the header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can configure multiple headers for each HTTP probe. The length of the *field-name* value plus the length of the *field-value* value plus 4 (for ":", space, and CRLF) cannot exceed 255 characters. This command is for HTTP probes.

Examples

This example shows how to configure a header field for the HTTP probe:

```
Cat6k-2(config-slb-probe-http)# header abacadabra
```

Related Commands

probe
show module csm probe

interval (probe submode)

To set the time interval between probes, use the **interval** command in the SLB probe configuration submode. To reset the time interval between probes to default, use the **no** form of this command.

interval *seconds*

no interval

Syntax Description

seconds	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe; the range is from 2 to 65535.

Defaults

The default value for the interval between probes is 120 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a probe interval of 150 seconds:

```
Cat6k-2(config-slb-probe-http)# interval 150
```

Related Commands

probe
show module csm probe

name (probe submode)

To configure a domain name for the DNS probe, use the **name** command in the SLB DNS probe configuration submode. To remove the name from the configuration, use the **no** form of this command.

name *domain-name*

no name

Syntax Description

domain-name	Domain name that the probe sends to the DNS server.

Defaults

This command has no default settings.

Command Modes

SLB DNS probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify the probe name that is resolved by the DNS server:

```
Cat6k-2(config-slb-probe-dns)# name astro
```

Related Commands

probe
show module csm probe

open (probe submode)

To set the time to wait for a TCP connection, use the **open** command in the SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode. To reset the time to wait for a TCP connection to default, use the **no** form of this command.

open *open-timeout*

no open

Syntax Description

open-timeout	Maximum number of seconds to wait for the TCP connection; the range is from 1 to 65535.

Defaults

The default value for the open timeout is 10 seconds.

Command Modes

SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is not used for any non-TCP probes, such as ICMP or DNS.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configure a time to wait for a TCP connection of 5 seconds:

```
Cat6k-2(config-slb-probe-http)# open 5
```

Related Commands

probe
show module csm probe

port (probe submode)

To configure an optional port for the DNS probe, use the **port** command in the SLB probe configuration submode. To remove the port from the configuration, use the **no** form of this command.

port *port-number*

no port

Syntax Description

port-number	Sets the port number.

Defaults

The default value for the port number is 0.

Command Modes

This command is available in all SLB probe configuration submodes except ICMP.

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When the port of a health probe is specified as 0, the health probe uses the configured port number from the real server (if a real server is configured) or the configured port number from the virtual server (if a virtual server is configured and no port is configured for the real server). The default port value is 0. For the ICMP probes, where there is no port number, the port value is ignored. The **port** command is available for all probe types except ICMP.

Examples

This example shows how to specify the port for the DNS server:

```
Cat6k-2(config-slb-probe-dns)# port 63
```

Related Commands

probe
show module csm probe

receive (probe submode)

To set the time to wait for a reply from a server, use the **receive** command in the SLB probe configuration submode. To reset the time to wait for a reply from a server to default, use the **no** form of this command.

receive *receive-timeout*

no receive

Syntax Description

receive-timeout	Number of seconds to wait for reply from a server; the range is from 1 to 65535.

Defaults

The default value for a receive timeout is 10 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types except TCP.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configure a time to wait for a reply from a server to 5 seconds:

```
Cat6k-2(config-slb-probe-http)# receive 5
```

Related Commands

probe
show module csm probe

recover (probe submode)

To set the number of consecutive responses that are sent before marking a failed server as healthy, use the **recover** command.

recover *recover_value*

no recover

Syntax Description

recover_value	Number of consecutive responses sent; the range is from 1 to 65535.

Defaults

The default value is 1.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types.

Examples

This example shows how to configure a time to wait for a reply from a server to 5 seconds:

```
Router(config-slb-probe-http)# recover 5
```

Related Commands

probe
show module csm probe

request (probe submode)

To configure the request method used by the HTTP probe, use the **request** command in the SLB HTTP probe configuration submode. To remove the request method from the configuration, use the **no** form of this command.

request [**method** {**get** | **head**}] [**url** *path*]

no request [**method** {**get** | **head**}] [**url** *path*]

Syntax Description

method get	(Optional) Configures a method for the probe request and directs the server to get this page.
method head	(Optional) Configures a method for the probe request and directs and directs the server to get only the header for this page.
url *path*	(Optional) A character string up to 255 characters specifying the URL path.

Defaults

The default path is /.
The default method is the **get** option.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The CSM supports only the **get** and **head** request methods. This command is for HTTP probes.

Examples

This example shows how to configure a request method for the probe configuration:

```
Cat6k-2(config-slb-probe-http)# request method head
```

Related Commands

probe
show module csm probe

retries (probe submode)

To set the number of failed probes that are allowed before marking the server failed, use the **retries** command in the SLB probe configuration submode. To reset the number of failed probes allowed before marking a server as failed to default, use the **no** form of this command.

retries *retry-count*

no retries

Syntax Description

retry-count	Number of probes to wait before marking a server as failed; the range is from 0 to 65535.

Defaults

The default value for retries is 3.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Note Set retries to 2 or more. If retries are set to 1, a single dropped probe packet will bring down the server. A setting of 0 places no limit on the number of probes that are sent. Retries are sent until the system reboots.

Examples

This example shows how to configure a retry count of 3:

```
Cat6k-2(config-slb-probe-http)# retries 3
```

Related Commands

probe
show module csm probe

script (probe submode)

To create a script for a probe, use the **script** command.

script *script_name*

Syntax Description

script_name	Specifies a probe script.

Defaults

This command has no default settings.

Command Modes

SLB probe script configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The script name should match a script in a configured script file.

Examples

This example shows how to create a script probe:

```
Cat6k-2(config-module-csm)# ip slb script file tftp://192.168.10.102/csmScripts
Cat6k-2(config-probe-script)# script echoProbe.tcl
Cat6k-2(config-probe-script)# interval 10
Cat6k-2(config-probe-script)# retries 1
Cat6k-2(config-probe-script)# failed 30
```

Related Commands

failed (probe submode)
interval (probe submode)
open (probe submode)
probe
receive (probe submode)
retries (probe submode)
script file
show module csm probe

real

To identify a real server that is a member of the server farm, and then enter the real server configuration submode, use the **real** command in the SLB serverfarm configuration submode. To remove the real server from the configuration, use the **no** form of this command.

real *ip-address* [*port*] [**local**]

no real *ip-address* [*port*]

Syntax Description

ip-address	Real server IP address.
port	(Optional) Port translation for the real server; the range is from 1 to 65535.
local	(Optional) Specifies that the real server is the SSL daughter card.

Defaults

The default is no port translation for the real server.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 4.1(3)	The local keyword was added to support the SSL daughter card.
CSM-S release 1.1(1)	This command was introduced and the local keyword was added.

Usage Guidelines

The IP address that you supply provides a load-balancing target for the CSM. This target can be any IP addressable object. For example, the IP addressable object may be a real server, a firewall, or an alias IP address of another CSM.

You can configure a real server as follows:

- **no inservice**—Using the **no inservice** command in the real server submode, the CSM is specified as out of service. There is no sticky and no new connections being applied.

Note If you specify **no inservice**, the CSM does not remove open connections. If you want to remove open connections. you must perform that task manually using the **clear module csm** *slot* **conn** command.

- **inservice**—Using the **inservice** command in the real server submode, the CSM is specified as in service. Sticky is allowed and new connections to the module can be made.
- **inservice standby**—Specifies that when in standby mode, the real server only accepts connections when the primary real server has failed.

Examples

This example shows how to identify a real server and enter the real server submode:

```
Cat6k-2(config-slb-sfarm)# real 102.43.55.60
Cat6k-2(config-slb-real)#
```

Related Commands

inservice (real server submode)
script task
show module csm real
show module csm serverfarm

backup real (real server submode)

To apply new connections to real servers when a primary server is down, use the **backup real** command in the SLB real server configuration submode. To remove a real server from service, use the **no** form of this command.

backup real {*ip* | **name** *name*} [*port*]

no backup real

Syntax Description

ip	Specifies the backup server's IP address.
name *name*	Specifies the real server name.
port	(Optional) Specifies the port where the backup real server is located.

Defaults

This command has no default settings.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

A weight of 0 is now allowed for graceful shutdown of existing connections. The **backup real** command can be used in these situations where a server farm is specified:

- Directly under a virtual server.
- In a policy and then associated to a virtual server.

Examples

This example shows how to enable a real server:

```
Cat6k-2(config-slb-real)# backup real 10.2.2.1 3
Cat6k-2(config-slb-real)#
```

Related Commands

failaction (serverfarm submode)
real (static NAT submode)
show module csm real

health probe (real server submode)

To configure a probe for the real server, use the **health probe** command in the SLB real server configuration submode. To remove the probe from the configuration, use the **no** form of this command.

health probe *probe-name* **tag** *string*

no health probe

Syntax Description

probe-name	Names the probe.
tag	Specifies a tag for the probe.
string	Specifies a string to identify the probe.

Defaults

This command has no default values.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure a probe for a server:

```
Cat6k-2(config-slb-sfarm)# real 102.2.2.1
Cat6k-2(config-slb-real)# health probe mission tag 12345678
```

Related Commands

real
show module csm real

inservice (real server submode)

To enable the real servers, use the **inservice** command in the SLB real server configuration submode. To remove a real server from service, use the **no** form of this command.

inservice [**standby**]

no inservice

Syntax Description

standby	(Optional) Specifies that when in standby mode, the real server only accepts connections when the primary real server has failed.

Defaults

The real server is not in service.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.2(1)	This command was modified for firewall load-balancing (FWLB) reassignment.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When you specify the **no inservice** command, the CSM will not remove open connections. To remove open connections, you must remove them using the **clear module csm** *slot* **connection** command.

The CSM performs graceful server shutdown when a real server is taken out of service when you enter the **no inservice** command. This command stops all new sessions from being load balanced to the specified real server while allowing existing sessions to complete or time out. New sessions are load balanced to other servers in the server farm for that virtual server.

This example shows how to remove a real server from service:

```
Router(config-slb-real)# no inservice
```

Examples

This example shows how to enable a real server:

```
Cat6k-2(config-slb-sfarm)# real 10.2.2.1
Cat6k-2(config-slb-real)# inservice
```

Related Commands

real
show module csm real

maxconns (real server submode)

To limit the number of active connections to the real server, use the **maxconns** command in the SLB real server configuration submode. To change the maximum number of connections to its default value, use the **no** form of this command.

maxconns *max-conns*

no maxconns

Syntax Description

max-conns	Maximum number of active connections on the real server at any time; the range is from 1 to 4294967295.

Defaults

The default value is the maximum value or infinite (not monitored).

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When you specify the **minconns** command, you must also specify the **maxconns** command. In all releases, when the MINCONNS value is set, once a real server has reached the maximum connections (MAXCONNS) state, no additional session is balanced to it until the number of open sessions to that real server falls below MINCONNS.

Examples

This example shows how to limit the connections to a real server:

```
Cat6k-2(config-slb-sfarm)# real 10.2.2.1
Cat6k-2(config-slb-real)# maxconns 4000
```

Related Commands

minconns (real server submode)
real
show module csm real

minconns (real server submode)

To establish a minimum connection threshold for the real server, use the **minconns** command in the SLB real server configuration submode. To change the minimum number of connections to the default value, use the **no** form of this command.

minconns *min-cons*

no minconns

Syntax Description

min-cons	Minimum number of connections allowed on the real server; the range is from 0 to 4294967295.

Defaults

The default value is the set minumum number of connections.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When the threshold of the **maxconns** command is exceeded, the CSM stops sending connections until the number of connections falls below the **minconns** command threshold. This value must be lower than the maximum number of connections configured by the **maxconns** command. When you specify the **minconns** command, you must also specify the **maxconns** command.

In all releases, when the MINCONNS value is set, once a real server has reached the maximum connections (MAXCONNS) state, no additional session is balanced to it until the number of open sessions to that real server falls below MINCONNS.

Examples

This example shows how to establish a minimum connection threshold for a server:

```
Cat6k-2(config-slb-sfarm)# real 102.2.2.1
Cat6k-2(config-slb-real)# minconns 4000
```

Related Commands

maxconns (real server submode)
real
show module csm real

redirect-vserver (real server submode)

To configure a real server to receive traffic redirected by a redirect virtual server, use the **redirect-vserver** command in the SLB real server configuration submode. To specify that traffic is not redirected to the real server, use the **no** form of this command.

redirect-vserver *name*

no redirect-vserver

Syntax Description

name	Name of the virtual server that has its requests redirected.

Defaults

Traffic is not redirected to the server.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Mapping real servers to redirect virtual servers provides persistence for clients to real servers across TCP sessions. Before using this command, you must create the redirect virtual server in serverfarm submode with the **redirect-vserver** command.

Examples

This example shows how to map a real server to a virtual server:

```
Cat6k-2(config-slb-sfarm)#   real 10.2.2.1
Cat6k-2(config-slb-real)# redirect-vserver timely
```

Related Commands

real
redirect-vserver
show module csm real
show module csm vserver redirect

weight (real server submode)

To configure the capacity of the real servers in relation to the other real servers in the server farm, use the **weight** command in the SLB real server configuration submode. To change the server's weight to its default capacity, use the **no** form of this command.

weight *weighting-value*

no weight

Syntax Description

weighting-value	Value to use for the server farm predictor algorithm; the range is from 0 to 100.

Defaults

The weighting value default is 8.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure the weight of a real server:

```
Cat6k-2(config-slb-sfarm)#   real 10.2.2.1
Cat6k-2(config-slb-real)# weight 8
```

Related Commands

predictor (serverfarm submode)
real
show module csm real

redirect-vserver

To specify the name of a virtual server to receive traffic redirected by the server farm, and then enter redirect virtual server configuration submode, use the **redirect-vserver** command. To remove the redirect virtual server, use the **no** form of this command.

redirect-vserver *name*

no redirect-vserver *name*

Syntax Description

name	Name of the virtual server to receive traffic redirected by the server farm; the virtual server name can be no longer than 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to name the virtual server:

```
Cat6k-2(config-slb-sfarm)#   redirect-vserver quantico
```

Related Commands

real
redirect-vserver (real server submode)
script task
show module csm serverfarm
show module csm vserver redirect

advertise (redirect virtual server submode)

To allow the CSM to advertise the IP address of the virtual server as the host route, use the **advertise** command in the SLB redirect virtual server configuration mode. To stop advertising the host route for this virtual server, use the **no** form of this command.

advertise [active]

no advertise

Syntax Description

active	(Optional) Allows the CSM to advertise the IP address of the virtual server as the host route.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Without the active option, the CSM always advertises the virtual server IP address whether or not there is any active real server attached to this virtual server.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
Cat6k-2(config-slb-redirect-vs)# advertise 10.5.2.1 exclude
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

client (redirect virtual server submode)

To restrict which clients are allowed to use the redirect virtual server, use the **client** command in the SLB redirect virtual server configuration mode. To remove the client definition from the configuration, use the **no** form of this command.

client *ip-address* [*network-mask*] [**exclude**]

no client *ip-address* [*network-mask*]

Syntax Description

ip-address	Client's IP address.
network-mask	(Optional) Client's IP mask.
exclude	(Optional) Specifies that the IP address is disallowed.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The network mask is applied to the source IP address of incoming connections and the result must match the IP address before the client is allowed to use the virtual server. If you do not specify the **exclude** option, the IP address and network mask combination is allowed.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
Cat6k-2(config-slb-redirect-vs)# client 10.5.2.1 exclude
```

Related Commands

advertise (virtual server submode)
client-group (policy submode)
show module csm vserver redirect

idle (redirect virtual server submode)

To specify the connection idle timer duration, use the **idle** command in the SLB redirect virtual server configuration submode. To disable the idle timer, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	SLB connection idle timer in seconds; the range is from 4 to 65535.

Defaults

The default is 3600.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify the connection idle timer duration:

```
Cat6k-2(config-slb-redirect-vs)# idle 7
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

inservice (redirect virtual server submode)

To enable the real server for use by the CSM, use the **inservice** command in the SLB redirect virtual server configuration submode. If this command is not specified, the virtual server is defined but not used. To disable the virtual server, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The virtual server is disabled.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable a redirect virtual server for use by the CSM:

```
Cat6k-2(config-slb-redirect-vs)# inservice
```

Related Commands

advertise (virtual server submode)
redirect-vserver
show module csm vserver redirect

replicate csrp (redirect virtual server submode)

To enable connection redundancy, use the **replicate csrp** command in the SLB redirect virtual server configuration submode. To remove connection redundancy, use the **no** form of this command.

replicate csrp

no replicate csrp

Syntax Description

This command has no keywords or arguments.

Defaults

Connection redundancy is removed.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable connection redundancy:

```
Cat6k-2(config-slb-redirect-vs)# replicate csrp
```

Related Commands

show module csm vserver redirect
vserver

ssl (redirect virtual server submode)

To redirect an HTTP request to either HTTPS (SSL) or the FTP service, use the **ssl** command in the SLB redirect virtual server configuration submode. To reset the redirect of an HTTP request to an HTTP service, use the **no** form of this command.

ssl {**https** | **ftp** | *ssl-port-number*}

no ssl

Syntax Description

https	Specifies secure HTTP service.
ftp	Specifies FTP service.
ssl-port-number	SSL port number; the range is from 1 to 65535.

Defaults

HTTP service.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable SSL forwarding:

```
Cat6k-2(config-slb-redirect-vs)# ssl 443
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

virtual (redirect virtual server submode)

To specify the virtual server's IP address, the protocol used for traffic, and the port the protocol is using, use the **virtual** command in SLB redirect virtual server configuration submode. To reset the virtual server to its defaults, use the **no** form of this command.

virtual *v_ipaddress* **tcp** *port*

no virtual *v_ipaddress*

Syntax Description

v_ipaddress	Redirect virtual server's IP address.
tcp	Specifies the protocol used for redirect virtual server traffic.
port	Port number used by the protocol.

Defaults

The default IP address is 0.0.0.0, which prevents packet forwarding.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify the virtual server's IP address, the protocol for redirect virtual server traffic, and the port number used by the protocol:

```
Cat6k-2(config-slb-redirect)# virtual 130.32.44.50 tcp 80
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

vlan (redirect virtual server submode)

To define which source VLANs can be accessed on the redirect virtual server, use the **vlan** command in the SLB redirect virtual server submode. To remove the VLAN, use the **no** form of this command.

vlan {*vlan-number* | **all**}

no vlan

Syntax Description

vlan-number	The VLAN that the virtual server can access.
all	Specifies that all VLANs are accessed by the virtual server.

Defaults

The default is all VLANs are accessed.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify a VLAN for redirect virtual server access:

```
Cat6k-2(config-slb-redirect-vs)# vlan 5
```

Related Commands

show module csm sticky
show module csm vserver redirect
sticky
sticky-group (policy submode)

webhost backup (redirect virtual server submode)

To specify a backup string sent in response to HTTP requests, use the **webhost backup** command in SLB redirect virtual server configuration submode. To disable the backup string, use the **no** form of this command.

webhost backup *backup-string* [**301** | **302**]

no webhost backup

Syntax Description

backup-string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Specifies the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Specifies the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used in situations where the redirect virtual server has no available real servers. The **301** value or **302** value is used to specify the redirect code. The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Examples

This example shows how to specify a backup string that is sent in response to HTTP requests:

```
Cat6k-2(config-slb-redirect-vs)# webhost backup www.mybackup.com%p 301
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

webhost relocation (redirect virtual server submode)

To specify a relocation string sent in response to HTTP requests, use the **webhost relocation** command in the SLB redirect virtual server configuration submode. To disable the relocation string, use the **no** form of this command.

webhost relocation *relocation string* [**301** | **302**]

no webhost relocation

Syntax Description

relocation string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Specifies the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Specifies the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Examples

This example shows how to specify a relocation string that is sent in response to HTTP requests:

```
Cat6k-2(config-slb-redirect-vs)# webhost relocation www.myhome1.com%p 301
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

reverse-sticky

To ensure that the CSM switches connections in the opposite direction and back to the original source, use the **reverse-sticky** command. To remove the reverse sticky option from the policy or the default policy of a virtual server, use the **no** form of this command.

reverse-sticky *group-id*

no reverse-sticky

Syntax Description

group-id	Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.

Defaults

The default is that the reverse sticky option is not connected. Sticky connections are not tracked. The group ID default is 0.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.1(1)	The **IP reverse-sticky** command is introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The sticky feature is not used for other virtual servers.

Examples

This example shows how to set the IP reverse-sticky feature:

```
Cat6k-2(config-module-csm)# vserver PUBLIC_HTTP
Cat6k-2(config-slb-vserver)# reverse-sticky 60
```

Related Commands

show module csm sticky
show module csm vserver redirect
sticky
sticky-group (policy submode)

script file

To load scripts from a script file to the CSM, use the **script file** command. To remove the script file command from the configuration, use the **no** form of this command.

script file {*file-url* | *bootflash:* | *const_nvram:* | *disk0:* | *flash:* | *ftp:* | *null:* | *nvram:* | *rcp:* | *slot0:* | *sup-bootflash:* | *sup-microcode:* | *sup-slot0:* | *system:* | *tftp:*}

no script file

Syntax Description

file-url	Sets the location of the script file to a URL.
bootflash:	Sets the standard Cisco IOS file name, such as bootflash:webprobe.tcl.
const_nvram:	Sets the location of the script file to the switch NVRAM.
disk0:	Sets the location of the script file on the CSM hard disk.
flash:	Sets the location of the script file to the CSM flash memory.
ftp:	Sets the location of the script file to an FTP location.
null:	Sets the location of the script file to NULL.
nvram:	Sets the location of the script file to the NVRAM.
rcp:	Sets the location of the script file to the switch.
slot0:	Sets the location of the script file to the switch.
sup-bootflash:	Sets the location of the script file to the switch supervisor engine bootflash.
sup-microcode:	Sets the location of the script file to the switch supervisor engine microcode.
sup-slot0:	Sets the location of the script file to the switch supervisor engine.
system:	Sets the location of the script file to the switch.
tftp:	Sets the location of the script file to a TFTP location.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	**Modification**
CSM release 3.1(1)	This command was introduced.

Usage Guidelines

The file URL is a standard Cisco IOS file name such as bootflash:webprobe.tcl.

Examples

This example shows how to load scripts from a script file to the CSM:

```
Cat6k-2(config-module-csm)# script file file-url
```

Related Commands

show module csm script

script task

To run a standalone task, use the **script task** command. To remove the standalone task from the configuration, use the **no** form of this command.

script task 1-100 script name

no script task 1-100 script name

Syntax Description

1-100	Task ID that identifies a specific running script.
script name	Identifies the script by name.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.

Examples

This example shows how to run a standalone script:

```
Cat6k-2(config-module-csm)# script task 30 filerun
```

Related Commands

show module csm script

serverfarm

To identify a server farm, and then enter the serverfarm configuration submode, use the **serverfarm** command. To remove the server farm from the configuration, use the **no** form of this command.

serverfarm *serverfarm-name*

no serverfarm *serverfarm-name*

Syntax Description

serverfarm-name	Character string used to identify the server farm; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Use this command to enter the server farm configuration submode to configure the load-balancing algorithm (predictor), a set of real servers, and the attributes (NAT, probe, and bindings) of the real servers.

Examples

This example shows how to identify a server farm named PUBLIC and change the CLI to server farm configuration mode:

```
Cat6k-2(config-module-csm)# serverfarm PUBLIC
```

Related Commands

script task
serverfarm (policy submode)
show module csm serverfarm

bindid (serverfarm submode)

To assign a unique ID to allow the DFP agent to differentiate a real server in one server farm versus another server farm, use the **bindid** command in the SLB serverfarm configuration submode. To disable the bind identification, use the **no** form of this command.

bindid [*bind-id*]

no bindid

Syntax Description

bind-id	(Optional) Identification number for each binding; the range is from 0 to 65533.

Defaults

The default is 0.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The single real server is represented as multiple instances of itself, each having a different bind identification. DFP uses this identification to identify a given weight for each instance of the real server.

Examples

This example shows how to bind a server to multiple virtual servers:

```
Cat6k-2(config-slb-sfarm)# bindid 7
```

Related Commands

dfp
script task
show module csm serverfarm

description (serverfarm submode)

To add a description for the serverfarm, use the **description** command in the SLB serverfarm configuration submode. To remove the description, use the **no** form of this command.

description *line*

no description

Syntax Description

line	Description text.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Examples

This example shows how to add a description:

```
Cat6k-2(config-slb-sfarm)# description Backup Server Farm
```

Related Commands

failaction (serverfarm submode)

To set the behavior of connections when the real servers have failed, use the **failaction** command in the SLB serverfarm configuration submode. To disable the behavior of connections to real servers that have failed, use the **no** form of this command.

failaction {**purge** | **reassign**}

no failaction {**purge** | **reassign**}

Syntax Description

purge	Specifies that the connection is removed.
reassign	Specfies that the connection is reassigned to another real server.

Defaults

The default is that no action is taken.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

With this command enabled, connections to a real server in the server farm are purged or reassigned when the real server goes down. This feature is required for stateful firewall load balancing.

Examples

This example shows how to set the behavior of connections to real servers that have failed:

```
Cat6k-2(config-slb-sfarm)# failaction purge
```

Related Commands

backup real (real server submode)
dfp
inservice (real server submode)
script task
show module csm serverfarm

health (serverfarm submode)

To set the retry attempts to real servers that have failed, use the **health** command in the SLB serverfarm configuration submode. To disable the retries or the time to wait for connections to real servers that have failed, use the **no** form of this command.

health retries *count* **failed** *seconds*

no health

Syntax Description

retries	Specifies the number of tries to attempt to failed real servers.
count	Number of probes to wait before marking a server as failed; the range is from 0 to 65534.
failed	Specifies the time to wait to attempt retries to the real servers.
seconds	Time in seconds before retrying a failed server; the range is from 0 to 65535.

Defaults

There are no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set the behavior of connections to real servers that have failed:

```
Cat6k-2(config-slb-sfarm)# health retries 20 failed 200
```

Related Commands

dfp
script task
show module csm serverfarm

nat client (serverfarm submode)

To specify a set of client NAT pool addresses that should be used to perform the NAT function on clients connecting to this server farm, use the **nat client** command in SLB serverfarm configuration submode. To remove the NAT pool from the configuration, use the **no** form of this command.

nat client {*client-pool-name* | **static**}

no nat client

Syntax Description

client-pool-name	Client pool name.
static	Enables static NAT.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.2(1)	This command was modified to include the **static** option.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Use this command to enable client NAT. If client NAT is configured, the client address and port number in load-balanced packets are replaced with an IP address and port number from the specified client NAT pool. This client pool name must match the pool name entered from a previous **natpool** command.

Examples

This example shows how to specify NAT on the client:

```
Cat6k-2(config-slb-sfarm)# nat client whishers
```

Related Commands

natpool (module CSM submode)
nat server (serverfarm submode)
predictor (serverfarm submode)
script task
show module csm serverfarm
static

nat server (serverfarm submode)

To specify NAT to servers in this server farm, use the **nat server** command in SLB serverfarm configuration submode. To disable server NAT, use the **no** form of this command.

nat server [**source-mac**]

no nat server

Syntax Description

source-mac	(Optional) Specifies that the request is forwarded back to the source MAC address.

Defaults

Server NAT is enabled by default.

Command Modes

SLB server farm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 4.1(1)	The **source-mac** value is added.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Use this command to enable server NAT. If server NAT is configured, the server address and port number in load-balanced packets are replaced with an IP address and port number of one of the real servers in the server farm.

Note The **nat server** command has no effect when **predictor forward** is configured, because no servers can be configured.

The **source-mac** value encrypts traffic for the SSL service and is specific to SSL devices. The **source-mac** value sends the request back to the SSL device for encryption, the CSM load balances to the server through the SSL encryption. This value supports back end encruption.

Examples

This example shows how to specify NAT on the server:

```
Cat6k-2(config-slb-sfarm)# nat server
```

Related Commands

nat client (serverfarm submode)
predictor (serverfarm submode)
script task
show module csm serverfarm

predictor (serverfarm submode)

To specify the load-balancing algorithm for the server farm, use the **predictor** command in the SLB serverfarm configuration submode. To remove the load-balancing algorithm, use the **no** form of this command.

predictor {**roundrobin** | **leastconns** [**slowstart** *timer*] | **hash url** | **hash address** [**source** | **destination**] [*ip-netmask*] | **forward**]}

no predictor

Syntax Description

roundrobin	Selects the next servers in the list of real servers.
leastconns	Selects the server with the least number of connections.
slowstart *timer*	Specifies that the real server is in slow-start mode until the **slowstart** *timer* value expires or the conn_count is equal to that of the other real servers. Valid values are from 1 to 65535 seconds.
hash url	Selects the server using a hash value based on the URL.
hash address	Selects the server using a hash value based on the source and destination IP addresses.
source	(Optional) Selects the server using a hash value based on the source IP address.
destination	(Optional) Selects the server using a hash value based on the destination IP address.
ip-netmask	(Optional) Bits in the IP address to use for the hash. If not specified, 255.255.255.255 is assumed.
forward	(Optional) Tells the CSM to forward traffic in accordance with its internal routing tables.

Defaults

The default algorithm is round robin.

For the **leastconns** option, **slowstart** is disabled by default.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM-S release 2.1(1)	Changed the **ip-hash** to the **hash address source** keyword and added new keyword types of **hash address**, **hash address destination**, **hash url**, and **forward**. In addition, the **http-redirect** command is now hidden.
CSM-S release 2.1(1)	The REAL_SLOW_START_ENABLE variable was included to control the rate at which a real server ramps up and is put into service.
CSM-S release 2.1(1)	The **slowstart** *timer* keyword was included to control the rate at which a real server ramps up and is put into service.

Usage Guidelines

Use this command to define the load-balancing algorithm used in choosing a real server in the server farm. If you do not specify the **predictor** command, the default algorithm is **roundrobin**. Using the **no** form of this command changes the predictor algorithm to the default algorithm.

Note The **nat server** command has no effect when **predictor forward** is configured, because no servers can be configured.

The portion of the URL to hash is based on the expressions configured for the virtual server submode **url-hash** command.

No real servers are needed. The server farm is actually a route forwarding policy with no real servers associated with it.

Cache servers perform better using URL hash. However, the hash methods do not recognize weight for the real servers. The weight assigned to the real servers is used in the round-robin and least connection predictor methods. To create different weights for real servers, you can list multiple IP addresses of the cache server in the server farm. You can also use the same IP address with a different port number.

Note The only time the sequence of servers starts over at the beginning (with the first server) is when there is a configuration or server state change (either a probe or DFP agent).

When the least connection predictor is configured, a slow-start mechanism is implemented to avoid sending a high rate of new connections to the servers that have just been put in service. The real server with the fewest number of active connections will get the next connection request for the server farm with the leastconns predictor. A new environment variable, REAL_SLOW_START_ENABLE, controls the rate at which a real server ramps up when it put into service. The slow start ramping up is only for a server farm configured with the “least-conns” method.

The configurable range for this variable is 0 to 10. The setting of 0 disables the slowstart feature. The value from 1 to 10 specifies how fast the newly activated server should ramp up. The value of 1 is the slowest ramp-up rate. The value of 10 specifies that the CSM would assign more requests to the newly activated server. The value of 3 is the default value.

If the configuration value is N, the CSM assigns 2 ^ N (2 raised to the N power) new requests to the newly active server from the start (assuming no connections were terminated at that time). As this server finishes or terminates more connections, a faster ramping occurs. The ramp up stops when the newly activated server has the same number of current opened connections as the other servers in a server farm.

Examples

This example shows how to specify the load-balancing algorithm for the server farm:

```
Cat6k-2(config-module-csm)# serverfarm PUBLIC
Cat6k-2(config-slb-sfarm)# predictor leastconns
```

This example shows how to configure a server farm, named p1_nat, using the least-connections (**leastconns**) algorithm.

```
Router(config-module-csm)# serverfarm pl_nat
Router(config-slb-sfarm)# predictor leastconns
Router(config-slb-sfarm)# real 10.1.0.105
Router(config-slb-real)# inservice
Router(config-slb-sfarm)# real 10.1.0.106
Router(config-slb-real)# inservice
```

Related Commands

maxconns (owner submode)
minconns (real server submode)
nat client (serverfarm submode)
nat server (serverfarm submode)
script task
serverfarm (virtual server submode)
show module csm serverfarm

probe (serverfarm submode)

To associate a probe with a server farm, use the **probe** command in the SLB serverfarm configuration submode. To disable a specific probe, use the **no** form of this command.

probe *probe-name*

no probe *probe-name*

Syntax Description

probe-name	Probe name associated with the server farm.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Each server farm can be associated with multiple probes of the same or different protocols. Protocols supported by the CSM include HTTP, ICMP, TCP, FTP, SMTP, Telnet, and DNS.

Examples

This example shows how to associate a probe with a server farm:

```
Cat6k-2(config-slb-sfarm)# probe general
```

Related Commands

probe
script task
show module csm probe
show module csm serverfarm

retcode-map (serverfarm submode)

To assign a return code map to a server farm, use the **retcode-map** command in the SLB serverfarm configuration submode. To disable a specific probe, use the **no** form of this command.

retcode-map *retcodemap_name*

no retcode-map

Syntax Description

retcodemap_name	Return code map name associated with the server farm.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to associate a probe with a server farm:

```
Cat6k-2(config-slb-sfarm)# retcode-map return_stats
```

Related Commands

map retcode
script task
show module csm serverfarm

show module csm

To display information about the CSM module, use the **show module csm** command.

show module csm *slot* [*group-id*]

Syntax Description

slot	Slot where the CSM resides.
group-id	(Optional) Group ID to which the CSM belongs.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced as **show ip slb**.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display static data:

```
Cat6k-2# show module csm 4 7
```

Related Commands

module csm
real (static NAT submode)
static

show module csm arp

To display the CSM ARP cache, use the **show module csm arp** command.

show module csm *slot* **arp**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb arp**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot (for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the CSM ARP cache:

```
Cat6k-2# show module csm 4 arp

Internet Address  Physical Interface  VLAN      Type       Status
--------------------------------------------------------------------
 10.10.3.100      00-01-64-F9-1A-02   0         VSERVER    local
 10.10.3.1        00-D0-02-58-B0-00   11        GATEWAY    up(0 misses)
 10.10.3.2        00-30-F2-71-6E-10   11/12     --SLB--    local
 10.10.3.10       00-D0-B7-82-38-97   12        REAL       up(0 misses)
 10.10.3.20       00-D0-B7-82-38-97   12        REAL       up(0 misses)
 10.10.3.30       00-D0-B7-82-38-97   12        REAL       up(0 misses)
 10.10.3.40       00-00-00-00-00-00   12        REAL       down(1 misses)
```

Related Commands

arp
module csm

show module csm capp

To display the CSM Content Application Peering Protocol (CAPP) configuration and statistics, use the **show module csm capp** command.

show module csm capp [**udp**] [**details**]

Syntax Description

udp	(Optional) Restricts output to UDP CAPP.
details	(Optional) Displays the client security options list.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the CSM CAPP configuration for UDP:

```
Cat6k-2# show module csm 4 capp
CAPP UDP Info
Port:5002, Allow non-secure:No
Transmit Frames:1762
Transmit Bytes: 1959344
Transmit Errors:0
Receive Frames: 1762
Receive Bytes:  1938200
Receive Errors: 0

Cat6k-2# show module csm 4 capp detail
CAPP UDP Info
Port:5002, Allow non-secure:No
Transmit Frames:1763
Transmit Bytes: 1960456
Transmit Errors:0
Receive Frames: 1763
Receive Bytes:  1939300
Receive Errors: 0
Security Options
IP address      Type    Secret
------------------------------------------------
10.3.0.2        MD5     test

Cat6k-2# show module csm 4 capp udp
CAPP UDP Info
Port:5002, Allow non-secure:No
Transmit Frames:1764
Transmit Bytes: 1961568
Transmit Errors:0
Receive Frames: 1764
Receive Bytes:  1940400
Receive Errors: 0

Cat6k-2# show module csm 4 capp udp detail
CAPP UDP Info
Port:5002, Allow non-secure:No
Transmit Frames:1764
Transmit Bytes: 1961568
Transmit Errors:0
Receive Frames: 1764
Receive Bytes: 1961568
Receive Errors: 0
Security Options
IP address      Type    Secret
------------------------------------------------
10.3.0.2        MD5     test
```

Related Commands

capp udp
module csm

show module csm conns

To display active connections, use the **show module csm conns** command.

show module csm *slot* **conns** [**vserver** *virtserver-name*] [**client** *ip-address*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
conns	Specifies the connections.
vserver	(Optional) Specifies the connections associated with a particular virtual server.
virtserver-name	(Optional) Name of the virtual server to be monitored.
client	(Optional) Specifies the connections associated with a particular client IP address.
ip-address	(Optional) IP address of the client to be monitored.
detail	(Optional) Specifies detailed connection information.

Defaults

If no options are specified, the command displays output for all active connections.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb conns**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot (for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The following connection state definitions are displayed in the output of this command.

State	Explanation
INIT	No TCP state available, but session received.
CLOSING	Received both client and server FINs, waiting for ACK of last FIN.
ESTAB	Client and server side connections established, balance decision made Non-TCP flows immediately transition to this state.
SYNCLINET	Client sent SYN, the CSM has sent SYN_ACK, waiting for ACK.
SYNBOTH	Client side connection established, sent SYN to server.
FINCLIENT	Received a FIN from client, waiting for server FIN.
FINSERVER	Received a FIN from server, waiting for client FIN.

State	Explanation
SYN_SRV	On a persistent Layer 7 connection (where the CSM parses each GET and eventually remaps the connection in the backend), if the load-balancing decision has selected a different server, the CSM has sent its SYN to the new server and is waiting on a server SYN_ACK from the new server.
REQ_WAIT	On a persistent Layer 7 connection, the CSM has already load balanced at least one request, and is now waiting for the next request.

Examples

This example shows how to display active connection data:

```
Cat6k-2# show module csm 4 conns
    prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80         ESTAB

In  TCP  11   100.100.100.2:1755    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80         ESTAB

Cat6k-2# show module csm 4 conns detail

    prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80         ESTAB
    vs = WEB_VIP, ftp = No, csrp = False

In  TCP  11   100.100.100.2:1755    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80         ESTAB
    vs = WEB_VIP, ftp = No, csrp = False
```

Related Commands

module csm

show module csm dfp

To display DFP agent and manager information, such as passwords, timeouts, retry counts, and weights, use the **show module csm dfp** command.

show module csm *slot* **dfp** [**agent** [**detail** | *ip-address port*] | **manager** [*ip_addr*] | **detail** | **weights**]

Syntax Description

slot	Slot where the CSM resides.
agent	(Optional) Specifies information about a DFP agent.
detail	(Optional) Specifies all data available.
ip_address	(Optional) Agent IP address.
port	(Optional) Agent port number.
manager	(Optional) Specifies the agent and manager connection state and statistics, and the load and health metric sent to DFP manager.
ip_addr	(Optional) IP address of reported weights.
detail	(Optional) Specifies all data available.
weights	(Optional) Specifies information about weights assigned to real servers for load balancing.

Defaults

If no options are specified, the command displays summary information.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb dfp**.
CSM release 2.1(1)	Added the virtual server weight display information to report to the DFP manager. This command was changed to **show module csm** *slot (for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows all available DFP data:

```
Cat6k-2# show module csm 4 dfp detail
```

This example shows information about weights:

```
Cat6k-2# show module csm 4 dfp weights
```

This example, with no options specified, shows summary information:

```
Cat6k-2# show module csm 4 dfp
```

Related Commands

agent (DFP submode)
dfp
manager (DFP submode)
module csm

show module csm ft

To display statistics and counters for the CSM fault-tolerant pair, use the **show module csm ft** command.

show module csm *slot* **ft** [**detail**]

Syntax Description

slot	Slot where the CSM resides.
detail	(Optional) Displays more detailed information.

Defaults

No values are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb ft**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **ft** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the statistics and counters for the CSM fault-tolerant pair:

```
Cat6k-2# show module csm 4 ft
FT group 2, vlan 30
 This box is active
 priority 10, heartbeat 1, failover 3, preemption is off
```

Related Commands

ft group
module csm

show module csm map

To display information about URL maps, use the **show module csm map** command.

show module csm *slot* **map** [**url** | **cookie** | **header** | **retcode**] [**name** *map-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
url	(Optional) Specifies only the URL map configuration.
cookie	(Optional) Specifies only the cookie map configuration.
header	(Optional) Specifies only the header map configuration.
retcode	(Optional) Specifies only the return code map configuration.
name	(Optional) Specifies the named map.
map-name	(Optional) Map name to display.
detail	(Optional) Specifies all data available.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb map**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **map** *(for* **ip slb mode rp** *only)*. The header option is added for displaying only header maps.
CSM release 2.2(1)	This command was changed to include the **retcode** option.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display URL maps associated with a content switching policy:

```
Cat6k-2# show module csm 4 map url
URL map UHASH_UMAP
 COOKIE map UHASH_CMAP1
 COOKIE map UHASH_CMAP2

6k#show ip slb map detail
 URL map UHASH_UMAP rules:
  *aabb*

 COOKIE map UHASH_CMAP1 rules:
  name:foo  value:*asdgjasgdkjsdkgjsasdgsg*

 COOKIE map UHASH_CMAP2 rules:
  name:bar  value:*asdgjasgdkjsdkgjsasdgsg*
```

This example shows how to display return code maps:

```
Cat6k-2# show module csm 5 map retcode detail
 RETCODE map HTTPCODES rules:
  return codes:401 to 401  action:log     threshold:5  reset:120
  return codes:402 to 415  action:count   threshold:0  reset:0
  return codes:500 to 500  action:remove  threshold:3  reset:0
  return codes:503 to 503  action:remove  threshold:3  reset:0
```

Related Commands

map cookie
map header
map url
module csm

show module csm memory

To display information about memory use, use the **show module csm memory** command.

show module csm *slot* **memory** [**vserver** *vserver-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
vserver	(Optional) Specifies the virtual server configuration.
vserver-name	(Optional) Option to restrict output to the named virtual server.
detail	(Optional) Displays the memory information in detail.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb memory**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **memory** *(for* **ip slb mode rp** *only)*. The **detail** keyword no longer has an effect and is hidden or deprecated.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the memory usage of virtual servers:

```
Cat6k-2# show module csm 4 memory
slb vserver      total bytes  memory by type
-----------------------------------------------------------------------
WEB_VIP          0             0         0
FTP_VIP          0             0         0
Total(s):                     0         0
Out of Maximum:               261424    261344
```

Related Commands

module csm
parse-length (virtual server submode)

show module csm natpool

To display NAT configurations, use the **show module csm natpool** command.

show module csm *slot* **natpool** [**name** *pool-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays a specific NAT pool.
pool-name	(Optional) NAT pool name string to display.
detail	(Optional) Lists the interval ranges currently allocated in the client NAT pool.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb natpool**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **natpool** *(for* **ip slb mode rp** *only).*
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display results of the default **show module csm** *slot* **natpool** command:

```
Cat6k-2# show module csm 4 natpool
nat client B  1.1(1).6  1.1(1).8  Netmask 255.255.255.0
       nat client A  1.1(1).1  1.1(1).5  Netmask 255.255.255.0
```

This example shows how to display results of the **show module csm** *slot* **natpool** command with the **detail** variable:

```
Cat6k-2# show module csm 4 natpool detail
nat client A  1.1(1).1  1.1(1).5  Netmask 255.255.255.0
     Start NAT        Last NAT         Count     ALLOC/FREE
     -------------------------------------------------------
     1.1(1).1:11001    1.1(1).1:16333    0005333   ALLOC
     1.1(1).1:16334    1.1(1).1:19000    0002667   ALLOC
     1.1(1).1:19001    1.1(1).5:65535    0264675   FREE
```

Related Commands

module csm
natpool (module CSM submode)

show module csm owner

To display the current connections count for the specified owner objects, use the **show module csm** *slot* **owner** command.

show module csm *slot* **owner** [**name** *owner-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays a specific owner object.
owner-name	(Optional) Owner object name string to display.
detail	(Optional) Lists the virtual servers in an owner group with the virtual server's state and current connections count.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Detailed information about an owner object lists the virtual servers in that group with each virtual server's state and current connections count.

The MAXCONNS state is displayed for a virtual server when the current connections counter is equal to the configured **maxconns** value. Counters for the number of connections dropped due to the virtual server being in this state are added. The **show module csm** *slot* **stats** and **show module csm** *slot* **vserver detail** command output displays these counters on a global and per-virtual server basis, respectively.

Examples

This example shows how to display results of the default **show module csm** *slot* **owner** command:

```
Cat6k-2# show module csm 4 owner
```

This example shows how to display results of the **show module csm** *slot* **owner** command with the **detail** variable:

```
Cat6k-2# show module csm 4 owner detail
```

Related Commands

module csm
owner (virtual server submode)

show module csm policy

To display a policy configuration, use the **show module csm policy** command.

show module csm *slot* **policy** [**name** *policy-name*]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays a specific policy.
policy-name	(Optional) Policy name string to display.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb policy**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **policy** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display a policy configuration:

```
Cat6k-2# show module csm 4 policy
policy:              PC1_UHASH_T1
sticky group:        20
serverfarm:          SF_UHASH_T1

policy:              PC1_UHASH_T2
sticky group:        30
serverfarm:          SF_UHASH_T2

policy:              PC1_UHASH_T3
url map:             UHASH_UMAP
serverfarm:          SF_UHASH_T3

policy:              PC1_UHASH_T4
cookie map:          UHASH_CMAP1
serverfarm:          SF_UHASH_T4

policy:              PC2_UHASH_T4
cookie map:          UHASH_CMAP2
serverfarm:          SF_UHASH_T4
Cat6k-2#
```

Related Commands

module csm
policy

show module csm probe

To display HTTP or ping probe data, use the **show module csm probe** command.

show module csm *slot* **probe** [**http** | **icmp** | **telnet** | **tcp** | **ftp** | **smtp** | **dns**] [**name** *probe_name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
http	(Optional) Displays information about the HTTP configuration.
icmp	(Optional) Displays information about the ICMP configuration.
telnet	(Optional) Displays information about the Telnet configuration.
tcp	(Optional) Displays information about the TCP configuration.
ftp	(Optional) Displays information about the FTP configuration.
smtp	(Optional) Displays information about the SMTP configuration.
dns	(Optional) Displays information about the DNS configuration.
name	(Optional) Displays information about the specific probe named.
probe_name	(Optional) Probe name to display.
detail	(Optional) Displays detailed information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb probe**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **probe** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display probe data:

```
Cat6k-2# show module csm 4 probe
probe             type      interval  retries  failed  open   receive
--------------------------------------------------------------------
PB_ICMP1          icmp      60        1        5              10
PB_HTTP1          http      60        1        10      10     10
PB_TCP1           tcp       60        1        10      10     10
PB_FTP1           ftp       60        1        10      10     10
PB_TELNET1        telnet    60        1        10      10     10
PB_SMTP1          smtp      60        1        10      10     10
```

Related Commands

module csm
probe (serverfarm submode)

show module csm probe script

To display probe script data, use the **show module csm probe script** command.

show module csm *slot* **probe script** [**name** *probe-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays information about the specific probe named.
probe-name	(Optional) Probe name to display.
detail	(Optional) Displays detailed information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display probe data:

```
Cat6k-2# show module csm 4 probe script detail
```

Related Commands

module csm
probe (serverfarm submode)
script (probe submode)

show module csm pvlan

To display information about the private VLAN status of the CSM, use the **show module csm real** command.

show module csm *slot* **pvlan**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Examples

This example shows how to display probe data:

```
Cat6k-2# show module csm 4 pvlan

 Primary     Secondary
 ----------- ----------------
 202         303
 202         440
```

Related Commands

module csm

show module csm real

To display information about real servers, use the **show module csm real** command.

show module csm *slot* **real** [**sfarm** s*farm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
sfarm	(Optional) Displays real servers for only a single server farm.
sfarm-name	(Optional) Name of the server farm to restrict output.
detail	(Optional) Displays detailed information.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb real**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **real** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows Cisco IOS SLB real server data:

```
Cat6k-2# show module csm 4 real
real                  server farm      weight  state          conns
-------------------------------------------------------------------
10.10.3.10            FARM1            20      OPERATIONAL    0
10.10.3.20            FARM1            16      OUTOFSERVICE   0
10.10.3.30            FARM1            10      OPERATIONAL    0
10.10.3.40            FARM1            10      FAILED         0

Cat6k-2# show mod csm 5 real detail
10.1.0.102, FARM1, state = OPERATIONAL
  Inband health:remaining retries = 3
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
10.1.0.101, FARM1, state = OPERATIONAL
  Inband health:remaining retries = 3
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
10.1.0.101, FARM2, state = OPERATIONAL
  conns = 2, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 2
  total conns established = 7, total conn failures = 0
```

Table 2-1 describes the fields in the display.

Table 2-1 show module csm real Command Field Information

Field	Description
real	Information about each real server is displayed on a separate line.
server farm	Name of the server farm associated to the real server.
weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
state	Current state of the real server: • OUTOFSERVICE—Removed from the load-balancing predictor lists. • FAILED—Removed from use by the predictor algorithms that start the retry timer. • OPERATIONAL—Functioning properly. • MAXCONNS • DFP_THROTTLED • PROBE_FAILED • PROBE_TESTING • TESTING—Queued for assignment. • READY_TO_TEST—Device functioning and ready to test.
conns	Number of connections.

Related Commands

module csm
real (static NAT submode)

show module csm real retcode

To display information about the return code configuration, use the **show module csm real retcode** command.

show module csm *slot* **real retcode** [**sfarm** s*farm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
sfarm	(Optional) Displays real servers for only a single server farm.
sfarm-name	(Optional) Name of the server farm to restrict output.
detail	(Optional) Displays detailed information.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 2.2.1	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows Cisco IOS SLB real server return code data:

```
Cat6k-2# show module csm 5 real retcode
10.1.0.101, FARM2, state = OPERATIONAL
  retcode-map = HTTPCODES
  retcode  action  count      reset-seconds  reset-count
  -----------------------------------------------------
  401      log     3          0              1
  404      count   62         0              0
  500      remove  1          0              0
```

Related Commands

module csm
real (static NAT submode)

show module csm script

To display the contents of all loaded scripts, use the **show module csm script** command.

show module csm *slot* **script** [**name** *full_file_URL*] [**code**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays information about a particular script.
full_file_URL	(Optional) Name of the script.
code	(Optional) Displays the contents of the script.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display script file contents:

```
Cat6k-2# show module csm 3 script name probe1 xxx
```

Related Commands

module csm
script file

show module csm script task

To display all loaded scripts, use the **show module csm script task** command.

show module csm *slot* **script task** [**index** *script-index*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
index	(Optional) Displays information about a particular script.
script-index	(Optional) Specifies the script index.
detail	(Optional) Displays the contents of the script.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display a running script:

```
Cat6k-2# show module csm 3 script
```

Related Commands

module csm
script file
script task
show module csm script

show module csm serverfarm

To display information about a server farm, use the **show module csm serverfarm** command.

show module csm *slot* **serverfarm** [**name** *serverfarm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Displays information about a particular server farm.
serverfarm-name	(Optional) Name of the server farm.
detail	(Optional) Displays detailed server farm information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb serverfarm**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **serverfarm** *(for* **ip slb mode rp** *only).*
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display server farm data:

```
Cat6k-2# show module csm 4 serverfarm
server farm      predictor    nat   reals   redirect  bind id
-------------------------------------------------------------
FARM1            RoundRobin   S     4       0         0
VIDEO_FARM       RoundRobin   S     5       0         0
AUDIO_FARM       RoundRobin   S     2       0         0
FTP              RoundRobin   S     3       0         0
```

Table 2-2 describes the fields in the display.

Table 2-2 show module csm serverfarm Command Field Information

Field	Description
server farm	Name of the server farm about which information is being displayed. Information about each server farm is displayed on a separate line.
predictor	Type of load-balancing algorithm used by the server farm.
nat	Shows whether server and client NAT is enabled.
reals	Number of real servers configured in the server farm.

Table 2-2 show module csm serverfarm Command Field Information (continued)

Field	Description
redirect	Number of redirect virtual servers configured in the server farm.
bind id	Bind ID configured on the server farm.

This example shows how to display only the details for one server farm:

```
Cat6k-2# show mod csm 5 serverfarm detail
FARM1, predictor = RoundRobin, nat = SERVER, CLIENT(CLNAT1)
 virtuals inservice:4, reals = 2, bind id = 0, fail action = none
 inband health config:retries = 3, failed interval = 200
 retcode map = <none>
 Real servers:
 10.1.0.102, weight = 8, OPERATIONAL, conns = 0
 10.1.0.101, weight = 8, OPERATIONAL, conns = 0
 Total connections = 0

FARM2, predictor = RoundRobin, nat = SERVER, CLIENT(CLNAT1)
 virtuals inservice:2, reals = 1, bind id = 0, fail action = none
 inband health config:<none>
 retcode map = HTTPCODES
 Real servers:
 10.1.0.101, weight = 8, OPERATIONAL, conns = 2
 Total connections = 2
```

Related Commands

module csm
serverfarm (virtual server submode)

show module csm static

To display information about server NAT configurations, use the **show module csm static** command.

show module csm *slot* **static** [**drop** | **nat** {*ip-address* | **virtual**}]

Syntax Description

slot	Slot where the CSM resides.
drop	(Optional) Displays information about real servers configured to drop connections.
nat	(Optional) Displays information about real servers configured to NAT.
ip-address	(Optional) IP address to which to NAT.
virtual	(Optional) Displays information about real servers configured to NAT virtual server IP addresses.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb static**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **static** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display static data:

```
Cat6k-2# show module csm 4 static nat
```

Related Commands

module csm
real (static NAT submode)
static

show module csm static server

To display information about actual servers that are having NAT performed, use the **show module csm static server** command.

show module csm *slot* **static server** [*ip-address*] [**drop** | **nat** {*ip-address* | **virtual**} | **pass-through**]

Syntax Description

slot	Slot where the CSM resides.
ip-address	(Optional) Option to limit output to a specified server address.
drop	(Optional) Displays information about real servers configured to drop connections.
nat	(Optional) Displays information about real servers configured to NAT.
ip-address	(Optional) IP address to NAT.
virtual	(Optional) Displays information about servers configured to NAT virtual server addresses.
pass-through	(Optional) Displays detailed information about real servers with no NAT configured.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb static server**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **static server** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display static server data:

```
Cat6k-2# show module csm 4 static server

Server           NAT Type
----------------------------------------------
10.10.3.10       NAT to 100.100.100.100
10.10.3.20       No NAT
10.10.3.30       NAT to 100.100.100.100
10.10.3.40       No NAT
Cat6k-1#
```

Related Commands

module csm
real (static NAT submode)
static

show module csm stats

To display SLB statistics, use the **show module csm stats** command.

show module csm *slot* **stats**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb stats**.
CSM-S release 2.1(1)	This command was changed to **show module csm** *slot* **stats** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The statistics counters are 32-bit.

Examples

This example shows how to display SLB statistics:

```
Cat6k-2# show module csm 4 stats
Connections Created:       180
Connections Destroyed:     180
Connections Current:       0
Connections Timed-Out:     0
Connections Failed:        0
Server initiated Connections:
      Created:0, Current:0, Failed:0
L4 Load-Balanced Decisions:180
L4 Rejected Connections:   0
L7 Load-Balanced Decisions:0
L7 Rejected Connections:
      Total:0, Parser:0,
      Reached max parse len:0, Cookie out of mem:0,
      Cfg version mismatch:0, Bad SSL2 format:0
L4/L7 Rejected Connections:
      No policy:0, No policy match 0,
      No real:0, ACL denied 0,
      Server initiated:0
Checksum Failures: IP:0, TCP:0
Redirect Connections:0,  Redirect Dropped:0
FTP Connections:           0
```

```
MAC Frames:
      Tx:Unicast:1506, Multicast:0, Broadcast:50898,
          Underflow Errors:0
      Rx:Unicast:2385, Multicast:6148349, Broadcast:53916,
          Overflow Errors:0, CRC Errors:0
```

Table 2-3 describes the fields in the display.

Table 2-3 show module csm stats Command Field Information

Field	Description
Connections Created	Number of connections that have been created since the last time counters were cleared.
Connections Destroyed	Number of connections that have been destroyed since the last time counters were cleared.

Related Commands

module csm

show module csm status

To display if the CSM is online, use the **show module csm status** command. If the CSM is online, this command shows the CSM chassis slot location and indicates if the configuration download is complete.

show module csm *slot* **status**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb status**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **status** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display CSM status:

```
Cat6k-2# show module csm 4 status
SLB Module is online in slot 4.
Configuration Download state:COMPLETE, SUCCESS
```

Related Commands

module csm

show module csm sticky

To display the sticky database, use the **show module csm sticky** command.

show module csm *slot* **sticky** [**groups** | **client** *ip_address*]

Syntax Description

slot	Slot where the CSM resides.
groups	(Optional) Displays all of the sticky group configurations.
client	(Optional) Displays the sticky database entries associated with a particular client IP address.
ip_address	(Optional) IP address of the client.

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb sticky**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **sticky** *(for* **ip slb mode rp** *only.*
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command only displays the database of the clients that are using IP stickiness; it does not show cookie or SSL entries.

Examples

This example shows how to display the sticky database:

```
Cat6k-2# show module csm 4 sticky groups
Group  Timeout  Type
------------------------------------------------------------
20     100      netmask 255.255.255.255
30     100      cookie foo
```

This example shows how to display the sticky configuration:

```
Cat6k-2# show module csm 4 sticky configuration
Group  CurrConns Timeout  Type
------------------------------------------------------------
7      12         2        ssl
```

Table 2-4 describes the fields in the display.

Table 2-4 show module csm stats Command Field Information

Field	Description
Group	Specifies the sticky group.
CurrConns	Number of sticky entries that are currently active.
Timeout	Specifies the timeout
Type	Specifies the connection identification.

Related Commands

module csm
sticky
sticky (virtual server submode)

show module csm tech-script

To display the status of a script, use the **show module csm tech-script** command.

show module csm *slot* **tech-script**

Syntax Description

slot	Slot where the CSM resides.

Defaults

If no options are specified, the command displays all information.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the technical support information for the CSM:

```
Cat6k-2# show module csm 4 tech-script
```

Related Commands

module csm

show module csm tech-support

To display technical support information for the CSM, use the **show module csm tech-support** command.

show module csm *slot* **tech-support** [**all** | **processor** *num* | **redirect** | **slowpath** | **probe** | **fpga** | **core-dump**]

Syntax Description

slot	Slot where the CSM resides.
all	(Optional) Displays all of the available statistics.
processor	(Optional) Displays the IXP statistics for the IXP identified by the *num* value.
num	(Optional) IXP number.
redirect	(Optional) Displays all of the HTTP redirect statistics.
slowpath	(Optional) Displays all of the slowpath statistics.
probe	(Optional) Displays all of the probe statistics.
fpga	(Optional) Displays all of the field programmable gate array (FPGA) statistics.
core_dump	(Optional) Displays all of the most recent statistics for the process (IXP or Power PC) that experienced a core dump.

Defaults

If no options are specified, the command displays all information.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb tech-support**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **tech-support** *(for* **ip slb mode rp** *only)*.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the technical support information for the CSM:

```
Cat6k-2# show module csm 4 tech-support ?
  all        All tech output
  core-dump  Most recent core dump
  fpga       FPGA info output
  ft         Fault Tolerance info output
  probe      Probe info output
  processor  Processor info output
  redirect   HTTP redirect info output
  slowpath   Slowpath info output
```

```
Cat6k-2# show module csm 4 tech-support processor 2
--------------------------------------------------------------
----------------------- TCP Statistics -----------------------
--------------------------------------------------------------
     Aborted rx                                 3350436013  66840864
     New sessions rx                            180         0
     Total Packets rx                           16940       0
     Total Packets tx                           0           0
     Packets Passthrough                        697         0
     Packets Dropped                            0           0
     Persistent OOO Packets Dropped             0           0
     Persistent Fastpath Tx                     0           0
     Total Persistent Requests                  0           0
     Persistent Same Real                       0           0
     Persistent New Real                        0           0

     Data Packets rx                            877         0
     L4 Data Packets rx                         877         0
     L7 Data Packets rx                         0           0
     Slowpath Packets rx                        7851        0
     Relinquish Requests rx                     8031        0

     TCP xsum failures                          0           0

     Session Mismatch                           0           0
     Session Reused while valid                 0           0
     Unexpected Opcode rx                       0           0
     Unsupported Proto                          0           0
     Session Queue Overflow                     0           0
     Control->Term Queue Overflow               0           0
     t_fifo Overflow                            0           0

     L7 Analysis Request Sent                   0           0
     L7 Successful LB decisions                 0           0
     L7 Need More Data decisions                0           0
     L7 Unsuccessful LB decisons                0           0
     L4 Analysis Request Sent                   180         0
     L4 Successful LB decisions                 180         0
     L4 Unsuccessful LB decisons                0           0

Transmit:
       SYN                                      0           0
       SYN/ACK                                  0           0
       ACK                                      0           0
       RST/ACK                                  0           0
       data                                     0           0
     Retransmissions:                          0           0
Receive:
       SYN                                      180         0
       SYN/ACK                                  0           0
       ACK                                      340         0
       FIN                                      0           0
       FIN/ACK                                  340         0
       RST                                      17          0
       RST/ACK                                  0           0
       data                                     0           0
```

```
Session Redundancy Standby:
     Rx Fake SYN                               0           0
     Rx Repeat Fake SYN                        0           0
     Rx Fake Reset                             0           0
     Fake SYN Sent to NAT                      0           0
     Tx Port Sync                              0           0
     Encap Not Found                           0           0
     Fake SYN, TCP State Invalid               0           0

Session Redundancy Active:
     L4 Requests Sent                          0           0
     L7 Requests Sent                          0           0
     Persistent Requests Sent                  0           0
     Rx Fake SYN                               0           0
     Fake SYN Sent to NAT                      0           0

     Session's torn down                       180         0
     Rx Close session                          1           0
     Slowpath(low  pri) buffer allocs          7843        0
     Slowpath(high pri) buffer allocs          8           0
     Small buffer allocs                       180         0
     Medium buffer allocs                      0           0
     Large buffer allocs                       0           0
     Session table allocs                      180         0

     Slowpath(low  pri) buffer alloc failures  0           0
     Slowpath(high pri) buffer alloc failures  0           0
     Small buffer allocs failures              0           0
     Medium buffer allocs failures             0           0
     Large buffer allocs failures              0           0
     Session table allocs failures             0           0

     Outstanding slowpath(low  pri) buffers    0           0
     Outstanding slowpath(high pri) buffers    0           0
     Outstanding small buffers                 0           0
     Outstanding medium buffers                0           0
     Outstanding large buffers                 0           0
     Outstanding sessions                      0           0
```

Related Commands

module csm

show module csm variable

To display the environmental variables in the configuration, use the **show module csm variable** command.

show module csm *slot* **variable** [**name** *name*] [**detail**]

Syntax Description

name *name*	(Optional) Displays the named variable information.
detail	(Optional) Displays the variable details.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

For a list of the CSM environmental variables, refer to the **variable (module CSM submode)** command description.

Examples

You can display the current set of CSM environmental variables by using the **show module csm** *slot* **variable** command:

```
Cat6k-2# show module csm 5 variable

variable                        value
----------------------------------------------------------------
ARP_INTERVAL                    300
ARP_LEARNED_INTERVAL            14400
ARP_GRATUITOUS_INTERVAL         15
ARP_RATE                        10
ARP_RETRIES                     3
ARP_LEARN_MODE                  1
ADVERTIZE_RHI_FREQ              10
DEST_UNREACHABLE_MASK           0xffff
HTTP_CASE_SENSITIVE_MATCHING    1
MAX_PARSE_LEN_MULTIPLIER        1
NAT_CLIENT_HASH_SOURCE_PORT     0

variable                        value
----------------------------------------------------------------
ROUTE_UNKNOWN_FLOW_PKTS         0
VSERVER_ICMP_ALWAYS_RESPOND     false
Cat6k-2#
```

You can display the details of a current set of CSM environmental variables by using the **show module csm** *slot* **variable detail** command:

```
Cat6k-2# show module csm 5 variable detail
Name: ARP_INTERVAL  Rights: RW
Value: 300
Default: 300
Valid values: Integer (15 to 31536000)
Description:
Time (in seconds) between ARPs for configured hosts
Name: ARP_LEARNED_INTERVAL  Rights: RW
Value: 14400
Default: 14400
Valid values: Integer (60 to 31536000)
Description:
Time (in seconds) between ARPs for learned hosts

Name: ARP_GRATUITOUS_INTERVAL  Rights: RW
Value: 15
Default: 15
Valid values: Integer (10 to 31536000)
Description:
Time (in seconds) between gratuitous ARPs

Name: ARP_RATE  Rights: RW
Value: 10
Default: 10
Valid values: Integer (1 to 60)
Description:
Seconds between ARP retries

Name: ARP_RETRIES  Rights: RW
Value: 3
Default: 3
Valid values: Integer (2 to 15)
Description:
Count of ARP attempts before flagging a host as down
!
```

show module csm vlan

To display the list of VLANs, use the **show module csm vlan** command.

show module csm *slot* **vlan** [**client** | **server** | **ft**] [**id** *vlan-id*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
client	(Optional) Displays only the client VLAN configuration.
server	(Optional) Displays only the server VLAN configuration.
ft	(Optional) Displays only the fault-tolerant configuration.
id	(Optional) Displays the VLAN.
vlan-id	(Optional) Displays the specified VLAN.
detail	(Optional) Displays the map configuration details.

Defaults

If no options are specified, the command displays information about all VLANs.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb vlan**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **vlan** *(for* **ip slb mode rp** *only).*
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the VLAN configurations:

```
Cat6k-2# show module csm 4 vlan

vlan   IP address       IP mask          type
---------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT
Cat6k-2#
Cat6k-2#
Cat6k-2# show module csm 4 vlan detail
vlan   IP address       IP mask          type
---------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
  GATEWAYS
  10.10.4.1
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT
```

Related Commands

vlan (virtual server submode)

show module csm vserver redirect

To display the list of virtual servers, use the **show module csm vserver redirect** command.

show module csm *slot* **vserver redirect**

Syntax Description

slot	Slot where the CSM resides.

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced as **show ip slb vserver redirect**.
CSM release 2.1(1)	This command was changed to **show module csm** *slot* **vserver redirect** *(for* **ip slb mode rp** *only).*
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the CSM virtual servers:

```
Cat6k-2# show module csm 4 vserver
slb vserver      prot  virtual                  vlan  state         conns
---------------------------------------------------------------------------
FTP_VIP          TCP   10.10.3.100/32:21        ALL   OUTOFSERVICE  0
WEB_VIP          TCP   10.10.4.100/32:80        ALL   OPERATIONAL   0
Cat6k-2#
Cat6k-2#
Cat6k-2# show module csm 4 vserver detail
FTP_VIP, state = OUTOFSERVICE, v_index = 3
  virtual = 10.10.3.100/32:21, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = ALL
  max parse len = 600, persist rebalance = TRUE
  conns = 0, total conns = 0
  Policy           Tot Conn     Client pkts  Server pkts
  ------------------------------------------------------
  (default)        0            0            0
WEB_VIP, state = OPERATIONAL, v_index = 4
  virtual = 10.10.4.100/32:80, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = ALL
  max parse len = 600, persist rebalance = TRUE
  conns = 0, total conns = 140
  Default policy:
    server farm = FARM1
    sticky:timer = 0, subnet = 0.0.0.0, group id = 0
  Policy           Tot Conn     Client pkts  Server pkts
  ------------------------------------------------------
  (default)        140          672          404
```

Related Commands

module csm

show module csm xml stats

To display a list of extensible markup language (XML) statistics, use the **show module csm xml stats** command.

show module csm xml stats

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the CSM XML statistics:

```
Cat6k-2# show module csm 4 xml stats
XML config:inservice, port = 80, vlan = <all>, client list = <none>
   connection stats:
     current = 0, total = 5
     failed = 2, security failed = 2
   requests:total = 5, failed = 2
```

Related Commands

xml-config

snmp enable traps slb ft

To enable or disable fault-tolerant traps, use the **snmp enable traps slb ft** command. To disable fault-tolerant traps, use the **no** form of this command.

snmp enable traps slb ft

no snmp enable traps slb ft

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

A fault-tolerant trap allows the CSM to send an SNMP trap when the CSM transitions from standby to active after detecting a failure in its fault tolerant peer.

Examples

This example shows how to enable fault tolerant traps:

```
Cat6k-2(config-module-csm)# snmp enable traps slb ft
```

static

To configure the server NAT behavior, and then enter the NAT configuration submode, use the **static** command. This command configures the CSM to support connections initiated by real servers. Both client NAT and server NAT can exist in the same configuration. To remove NAT from the CSM configuration, use the **no** form of this command.

static {**drop** | **nat** {**virtual** | *ip-address*}}

no static {**drop** | **nat** {**virtual** | *ip-address*}}

Syntax Description

drop	Drops connections from servers specified in static submode.
nat	Uses the server's virtual IP (VIP) to translate its source IP address.
virtual	Specifies that the configuration is for NAT.
ip-address	IP address to be used for NAT.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to configure the CSM to support connections initiated by the real servers:

```
Cat6k-2(config-module-csm)# static nat virtual
```

Related Commands

module csm
nat client (serverfarm submode)
show module csm static

real (static NAT submode)

To specify the address for a real server or the subnet mask for multiple real servers performing server NAT, use the **real** command in SLB static NAT configuration submode. To remove the address of a real server or the subnet mask of multiple real servers so they are no longer performing NAT, use the **no** form of this command.

real *real-ip-address* [*real-netmask*]

no real *real-ip-address* [*real-netmask*]

Syntax Description

real-ip-address	Real server IP address performing NAT.
real-netmask	(Optional) Range of real servers performing NAT. If not specified, the default is 255.255.255.255 (a single real server).

Defaults

This command has no default settings.

Command Modes

SLB static NAT configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify the address for a real server:

```
Cat6k-2(config-slb-static)# real 10.0.0.0 255.0.0.0
```

Related Commands

show module csm static
static

sticky

To ensure that connections from the same client that match the same SLB policy use the same real server on subsequent connections and enter the sticky submode, use the **sticky** command. To remove a sticky group, use the **no** form of this command.

sticky *sticky-group-id* {**netmask** *netmask* | **cookie** *nam*e [**insert**] | **ssl** | **header** *name* [**default** | **header** | **static**]} [**address** [**source** | **destination** | **both**]] [**timeout** *sticky-time*]

no sticky s*ticky-group-id*

Syntax Description

sticky-group-id	ID to identify the sticky group instance; the range is from 1 to 255.
netmask *netmask*	Specifies the network mask for IP stickiness.
cookie *name*	Specifies name of the cookie attached to the *sticky-group-id* value.
insert	(Optional) Specifies the cookie insert.
ssl	Specifies SSL stickiness.
header *name*	Specifies HTTP header stickiness.
address | **source** | **destination** **both**	Specifies the real server IP address for the source, or the destination, or both.
timeout *sticky-time*	(Optional) Specifies the sticky timer duration in minutes; the range is from 0 to 65535.

Defaults

The sticky time default value is 1440 minutes (24 hours).

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM-S release 2.1(1)	Changed the default timeout from 0 to 1440.
CSM release 4.1(1)	The **insert** keyword was added.
CSM release 4.2(1)	The **header** keyword was added.

Usage Guidelines

Specifying a net mask permits sticky connections based on the masked client IP address.

Use the sticky time option to ensure that connections from the same client that match the same SLB policy use the same real server. If you specify a nonzero value, the last real server that was used for a connection from a client is remembered for the *sticky-time* value after the end of the client's latest connection.

However, if the environment variable NO_TIMEOUT_IP_STICKY_ENTRIES is set to 1, then the sticky timer for a specific entry is reset from the point where the last session ends. This timeout policy applies to sessions using IP_Sticky only. Sessions using other forms of persistence (for example, cookie and url-hash) are not affected by this behavior.

New connections from the client to the virtual server initiated before the sticky time expires and that match SLB policy are balanced to the same real server that was used for the previous connection.

A sticky time of 0 means sticky connections are not tracked.

The cookie insert feature allows the CSM to insert a cookie in the Set-Cookie header in the HTTP response.

Examples

This example shows how to create an IP sticky group based on network mask address:

```
Cat6k-2(config-module-csm)# sticky 5 netmask 255.255.255.255 timeout 20
Cat6k-2(config-slb-sticky-ip)#
```

This example shows how to create an IP sticky group based on the HTTP header:

```
Cat6k-2(config-module-csm)# sticky 5 header header_name timeout 20
Cat6k-2(config-slb-sticky-header)#
```

This example shows how to configure the sticky environment variable

```
Router(config-module-csm)# variable NO_TIMEOUT_IP_STICKY_ENTRIES 1
```

Related Commands

cookie offset (sticky submode)
cookie secondary (sticky submode)
header (sticky submode)
sticky (virtual server submode)
sticky-group (policy submode)
show module csm sticky

cookie offset (sticky submode)

To maintain a connections persistence by specifying a portion of the cookie to use to "stick" the connection, use the **cookie offset** command in the sticky configuration submode. To remove the offset, use the **no** form of this command.

cookie offset *offset* [**length** *length*]

no cookie offset

Syntax Description

offset *offset*	Specifies the byte offset count. Range is from 0 to 3999.
length *length*	(Optional) Specifies the length of the portion of the cookie you are using. Range is from 1 to 4000.

Defaults

This command has no default settings.

Command Modes

Sticky configuration submode

Command History

Release	Modification
CSM release 4.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Specify the offset in bytes counting from the first byte of the cookie value. The length (in bytes) is the portion of the cookie you are using to maintain the sticky connection. These values are stored in the sticky tables.

Examples

This example shows how to specify a cookie offset and length:

```
Cat6k-2(config-slb-sticky-cookie)# cookie offset 20 length 66
```

Related Commands

cookie secondary (sticky submode)
show module csm sticky
sticky
sticky (virtual server submode)
sticky-group (policy submode)

cookie secondary (sticky submode)

To stick a connection based on an alternate cookie name appearing in the URL string, and add a secondary sticky entry, use the **cookie secondary** command in the name configuration submode. To remove a secondary sticky, use the **no** form of this command.

cookie secondary *name*

no cookie secondary

Syntax Description

name	Specifies a cookie name.

Defaults

This command has no default settings.

Command Modes

Sticky configuration submode

Command History

Release	Modification
CSM release 4.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used for the URL-cookie-learn feature. The secondary name may be the same as the primary name.

Examples

This example shows how to specify a secondary sticky entry:

```
Cat6k-2(config-slb-sticky-cookie)# cookie secondary ident2
```

Related Commands

show module csm sticky
sticky
sticky (virtual server submode)
sticky-group (policy submode)

header (sticky submode)

To stick a connection based on the contents of the HTTP header, use the **header** command in the sticky configuration submode.

header offset *value* **length** *value*

Syntax Description

offset *value*	Specifies the number of bytes to ignore from the start of the header. Valid values are from 0 to 3399.
length *value*	Specifies the number of bytes to parse in the header. Valid values are from 1 to 4000.

Defaults

The default offset value is 0.

The default length value is 4400.

Command Modes

Sticky configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Examples

This example shows how to configure the header offset and length:

```
Cat6k-2(config-slb-sticky-header)# header offset 5 length 500
```

Related Commands

sticky
show module csm sticky

static (sticky submode)

To add a static sticky entry, use the **static** command. To remove a sticky group, use the **no** form of this command.

static client source *ip-address* [**destination** *ip-address*] **real** *ip-address*

static cookie *value* **real** *ip-address*

static ssl *id* **real** *ip-address*

no static

Syntax Description

client *source ip-address*	Identifies the client source for thte sticky entry.
destination *ip-address*	(Optional) Specifies the destination IP address.
real *ip-address*	Identifies the real server.
cookie *value*	Identifies the cookie.
ssl *id*	Identifies SSL.

Defaults

This command has no default settings.

Command Modes

Sticky configuration submode

Command History

Release	Modification
CSM release 3.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to create an IP sticky group:

```
Cat6k-2(config-module-csm)# sticky 5 netmask 255.255.255.255 timeout 20
Cat6k-2(config-slb-sticky-ip)#
```

Related Commands

show module csm sticky
sticky
sticky (virtual server submode)
sticky-group (policy submode)

vserver

To identify a virtual server, and then enter the virtual server configuration submode, use the **vserver** command. To remove a virtual server from the configuration, use the **no** form of this command.

vserver *virtserver-name*

no vserver *virtserver-name*

Syntax Description

virtserver-name	Character string used to identify the virtual server; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.

Examples

This example shows how to identify a virtual server named PUBLIC_HTTP and change the CLI to virtual server configuration mode:

```
Cat6k-2(config-module-csm)#   vserver PUBLIC_HTTP
```

Related Commands

redirect-vserver
show module csm vserver redirect

advertise (virtual server submode)

To allow the CSM to advertise the IP address of the virtual server as the host route, use the **advertise** command in the SLB virtual server configuration mode. To stop advertising the host route for this virtual server, use the **no** form of this command.

advertise [**active**]

no advertise

Syntax Description

active	(Optional) Allows the CSM to advertise the IP address of the virtual server as host route.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Without the active option, the CSM always advertises the virtual server IP address whether or not there is any active real server attached to this virtual server.

Examples

This example shows how to restrict a client from using the virtual server:

```
Cat6k-2(config-slb-redirect-vs)# advertise 10.5.2.1 exclude
```

Related Commands

redirect-vserver
show module csm vserver redirect

client (virtual server submode)

To restrict which clients are allowed to use the virtual server, use the **client** command in the SLB virtual server configuration mode. To remove the client definition from the configuration, use the **no** form of this command.

client *ip-address* [*network-mask*] [**exclude**]

no client *ip-address* [*network-mask*]

Syntax Description

ip-address	Client's IP address.
network-mask	(Optional) Client's IP mask.
exclude	(Optional) Specifies that the IP address is disallowed.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The network mask is applied to the source IP address of incoming connections and the result must match the IP address before the client is allowed to use the virtual server. If exclude is not specified, the IP address and network mask combination is allowed.

Examples

This example shows how to restrict a client from using the virtual server:

```
Cat6k-2(config-slb-vserver)# client 10.5.2.1 exclude
```

Related Commands

advertise (virtual server submode)
client-group (policy submode)
ip access-list standard
show module csm vserver redirect

description (virtual server submode)

To add a description for the server farm, use the **description** command in the virtual server configuration submode. To remove the description, use the no form of this command.

description *line*

no description

Syntax Description

line	Description text.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release4.2(1)	This command was introduced.

Usage Guidelines

Examples

This example shows how to add a description:

```
Cat6k-2(config-slb-vserver)# description Backup Server Farm
```

Related Commands

vserver

domain (virtual server submode)

To set the domain name, use the **domain** command in the SLB virtual server configuration mode. To remove the domain name from the configuration, use the **no** form of this command.

domain *domain-name*

no domain *domain-name*

Syntax Description

domain-name	Client's domain name.

Defaults

There are no default values.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set a domain name:

```
Cat6k-2(config-slb-vserver)# domain cisco.com
```

Related Commands

advertise (virtual server submode)
capp udp

idle (virtual server submode)

To control the amount of time the CSM maintains connection information in the absence of packet activity, use the **idle** command in the SLB virtual server configuration submode. To change the idle timer to its default value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	Idle connection timer duration in seconds; the range is from 0 (connection remains open indefinitely) to 13500000.

Defaults

The default is 3600.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	The minimum value for *duration* was changed from 4 to 0.

Usage Guidelines

If you do not specify a duration value, the default value is applied.

Examples

This example shows how to specify an idle timer duration of 4000:

```
Cat6k-2(config-slb-vserver)# idle 4000
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect
advertise (virtual server submode)

inservice (virtual server submode)

To enable the virtual server for load balancing, use the **inservice** command in the SLB virtual server configuration submode. To remove the virtual server from service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no keywords or arguments.

Defaults

The virtual server is not in service.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable a virtual server for load balancing:

```
Cat6k-2(config-slb-vserver)# inservice
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

owner (virtual server submode)

To define an owner that may access the virtual server, use the **owner** command in the SLB virtual server submode. To remove the owner, use the **no** form of this command.

owner *owner-name* **maxconns** *number*

no owner maxconns

Syntax Description

owner-name	Name of the owner object.
maxconns	Sets the maximum number of connections for this owner.
number	Maximum number of connections.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify an owner for virtual server access:

```
Cat6k-2(config-slb-vserver)# owner madrigal maxconns 1000
```

Related Commands

advertise (virtual server submode)

parse-length (virtual server submode)

To set the maximum number of bytes to parse for URLs and cookies, use the **parse-length** command in the SLB virtual server configuration submode. To restore the default, use the **no** form of this command.

parse-length *bytes*

no parse-length

Syntax Description

bytes	Number of bytes; the range is from 1 to 4000.

Defaults

The default is 600.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to set the number of bytes to parse for URLs and cookies:

```
Cat6k-2(config-slb-vserver)# parse-length 1000
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

pending (virtual server submode)

To set the pending connection timeout, use the **pending** command in the SLB virtual server configuration submode. To restore the default, use the **no** form of this command.

pending *timeout*

no pending

Syntax Description

timeout	Seconds to wait before a connection is considered unreachable. Range is from 1 to 65535.

Defaults

The default pending timeout is 30 seconds.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.2(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command is used to prevent denial-of-service (DOS) attacks. The pending connection timeout sets the response time for terminating connections if a switch becomes flooded with traffic. The pending connections are configurable on a per-virtual-server basis.

Examples

This example shows how to set the number to wait for a connection to be made to the server:

```
Cat6k-2(config-slb-vserver)# pending 300
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

persistent rebalance (virtual server submode)

To enable or disable HTTP 1.1 persistence for connections in the virtual server, use the **persistent rebalance** command in the SLB virtual server configuration submode. To disable persistence, use the **no** form of this command.

persistent rebalance

no persistent rebalance

Syntax Description

This command has no keywords or arguments.

Defaults

Persistence is disabled.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable the HTTP 1.1 persistence:

```
Cat6k-2(config-slb-vserver)# persistent rebalance
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

replicate csrp (virtual server submode)

To enable connection redundancy, use the **replicate csrp** command in the SLB virtual server configuration submode. To disable connection redundancy, use the **no** form of this command.

replicate csrp {**sticky** | **connection**}

no replicate csrp {**sticky** | **connection**}

Syntax Description

sticky	Replicates the sticky database to the backup CSM.
connection	Replicates connections to the backup CSM.

Defaults

Connection redundancy is disabled.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Sticky and connection replication can be enabled or disabled separately. For replication to occur, you must enable SLB fault tolerance with the **ft group** command.

Examples

This example shows how to enable connection redundancy:

```
Cat6k-2(config-slb-vserver)# replicate csrp connection
```

Related Commands

advertise (virtual server submode)
show module csm vserver redirect

reverse-sticky (virtual server submode)

To ensure that the CSM switches connections in the opposite direction back to the original source, use the **reverse-sticky** command in the virtual server submode. To remove the reverse-sticky option from the policy or the default policy of a virtual server, use the **no** form of this command.

reverse-sticky *group-id*

no reverse-sticky

Syntax Description

group-id	Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.

Defaults

Reverse sticky is not enabled.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.1(1)	The **IP reverse-sticky** command is introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Sticky connections are not tracked. The group ID default is 0. The sticky feature is not used for other virtual servers. The network default is 255.255.255.255.

Examples

This example shows how to set the IP reverse-sticky feature:

```
Cat6k-2(config-module-csm)# vserver PUBLIC_HTTP
Cat6k-2(config-slb-vserver)# reverse-sticky 60
```

Related Commands

show module csm sticky
show module csm vserver redirect
sticky
sticky-group (policy submode)

serverfarm (virtual server submode)

To associate a server farm with a virtual server, use the **serverfarm** command in SLB virtual server configuration submode. To remove a server farm association from the virtual server, use the **no** form of this command.

serverfarm *primary_serverfarm* [**backup** *backup_serverfarm* [**sticky**] [**threshold outservice** *real_value* **inservice** *real_value*][**sticky**]

no serverfarm

Syntax Description

primary_serverfarm	Character string used to identify the server farm.
backup	(Optional) Sets the name of a backup server farm.
backup_serverfarm	(Optional) Backup server farm name.
sticky	(Optional) Associates the backup server farm with a virtual server.
threshold	(Optional) Configures the server farm health threshold.
outservice *real_value*	(Optional) Specifies the minimum number of active real servers required to remain as healthy. The outservice *value* must be lower than the inservice *real_value.*
inservice *real_value*	(Optional) Specifies the number of active real servers required for the server farm to be activated.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM-S release 1.1(1)	The backup server option was added to this command.
CSM-S release 2.1(1)	The **threshold outservice** *real_value* **inservice** *real_value* options were added to this command.

Usage Guidelines

The server farm name must match the server farm name specified in a previous module CSM submode **serverfarm** command.

The backup server farm can be associated with a policy. A primary server farm must be associated with that policy to allow the backup server farm to function properly. The backup server farm can have a different predictor option than the primary server. When the sticky option is used for a policy, then stickiness can apply to real servers in the backup server farm. Once a connection has been balanced to a server in the backup server farm, subsequent connections from the same client can be stuck to the same server even when the real servers in the primary server farm come back to the operational state. You may allow the sticky attribute when applying the backup server farm to a policy.

By default, the sticky option does not apply to the backup server farm. To remove the backup server farm, you can either use the **serverfarm** command without the backup option or use the **no serverfarm** command.

Examples

This example shows how to associate a server farm with a virtual server named PUBLIC_HTTP:

```
Cat6k-2(config-slb-vserver)# serverfarm PUBLIC_HTTP backup seveneleven sticky
```

Related Commands

advertise (virtual server submode)
serverfarm (policy submode)
show module csm vserver redirect

slb-policy (virtual server submode)

To associate a load-balancing policy with a virtual server, use the **slb-policy** command in the SLB virtual server configuration submode. To remove a policy from a virtual server, use the **no** form of this command.

slb-policy *policy-name* [**priority** *priority_value*]

no slb-policy *policy-name*

Syntax Description

policy-name	Policy associated with a virtual server.
priority *priority_value*	(Optional) Specifies the order in which the policy is to be executed. Valid values for *priority_value* are 1 (highest priority) through 12,287.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM-S release 2.1(1)	The **priority** keyword was introduced.

Usage Guidelines

Multiple load-balancing policies can be associated with a virtual server. URLs in incoming requests are parsed and matched against policies defined in the same order in which they are defined with this command. The policy name must match the name specified in a previous **policy** command.

Note If **priority** *priority_value* is not entered, policies are executed in the order in which they are entered. In this case, you should enter the highest priority policy first.

Examples

This example shows how to associate a policy with a virtual server:

```
Cat6k-2(config-slb-vserver)# slb-policy COOKIE-POLICY1 priority 2
```

Related Commands

advertise (virtual server submode)
policy
show module csm owner
show module csm vserver redirect

ssl-sticky (virtual server submode)

To allow SSL sticky operation, use the **ssl-sticky** command in the SLB virtual server configuration submode. To remove the SSL sticky feature, use the **no** form of this command.

ssl-sticky offset *X* **length** *Y*

no ssl-sticky

Syntax Description

offset	Specifies the SSL ID offset.
X	Sets the offset value.
length	Specifies the SSL ID length.
Y	Sets the length.

Defaults

Offset is 0 and length is 32.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This feature allows you to stick an incoming SSL connection based only on this special section of the SSL ID specified by the offset and length values. The **ssl-sticky** command was added to ensure that the CSM always load balances an incoming SSL connection to the SSL termination engine that generated that SSL ID.

Examples

This example shows how to associate a policy with a virtual server:

```
Cat6k-2(config-slb-vserver)# ssl-sticky offset 0 length 32
```

Related Commands

advertise (virtual server submode)
policy
show module csm owner
show module csm vserver redirect

status-tracking (virtual server submode)

To link virtual servers to create a virtual server dependency, use the **status-tracking** command. If a virtual server goes out of service, the specified dependent virtual server is taken out of service automatically.

status-tracking *vserver_name*

Syntax Description

vserver_name	Identifies the dependent virtual server.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Examples

This example shows how to specify SERVER2 as the dependent virtual server:

```
Router(config-module-csm)# vserver SERVER1
Router(config-slb-vserver)# status-tracking SERVER2
```

Related Commands

advertise (virtual server submode)

sticky (virtual server submode)

To ensure that connections from the client use the same real server, use the **sticky** command in the virtual server submode. To change the sticky timer to its default value and remove the sticky option from the virtual server, use the **no** form of this command.

sticky *duration* [***group*** *group-id*] [**netmask** *ip-netmask*] [**source** | **destination** | **both**]

no sticky

Syntax Description

duration	Sticky timer duration in minutes; the range is from 1 to 65535.
group	(Optional) Places the virtual server in a sticky group for connection coupling.
group-id	(Optional) Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.
netmask	(Optional) Specifies which part of the address should be used for stickiness.
ip-netmask	(Optional) Network that allows clients to be stuck to the same server.
source	(Optional) Specifies the source portion of the IP address.
destination	(Optional) Destination portion of the IP address.
both	(Optional) Specifies that both the source and destination portions of the IP address are used.

Defaults

The sticky option is not in the server.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 3.1(1)	The IP reverse-sticky optional parameters are introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Sticky connections are not tracked. The group ID default is 0. The sticky feature is not used for other virtual servers. The network default is 255.255.255.255.

The last real server that was used for a connection from a client is stored for the *duration* value after the end of the client’s latest connection. If a new connection from the client to the virtual server is initiated during that time, the same real server that was used for the previous connection is chosen for the new connection.

A nonzero sticky group ID must correspond to a sticky group previously created using the **sticky** command. Virtual servers in the same sticky group share sticky state information.

Examples

This example shows how to set the sticky timer duration and places the virtual server in a sticky group for connection coupling:

```
Cat6k-2(config-module-csm)# vserver PUBLIC_HTTP
Cat6k-2(config-slb-vserver)# sticky 60 group 3
```

Related Commands

advertise (virtual server submode)
reverse-sticky (virtual server submode)
show module csm sticky
show module csm vserver redirect
sticky
sticky-group (policy submode)

unidirectional (virtual server submode)

To select the traffic type and appropriate timeout value, use the **unidirectional** command in the SLB virtual server submode.

[**no** | **default**] **unidirectional**

Syntax Description

no	(Optional) Removes the traffic type and timeout values from the configuration.
default	(Optional) Specifies that the CSM selects the appropriate behavior (unidirectional or bidirectional) based on the protocol.

Defaults

The default is **default**.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The CSM selects the traffic type and the correct timeout behavior for that traffic. The current timeout value can be displayed using the **show module csm vserver detail** commands.

Examples

This example shows how to select the traffic type and the timeout behavior:

```
Cat6k-2(config-slb-vserver)# default unidirectional
```

Related Commands

show module csm vserver redirect

url-hash (virtual server submode)

To set the beginning and ending pattern of a URL to parse URLs for the URL hash load-balancing algorithm, use the **url-hash** command in the SLB virtual server configuration submode. To remove the hashing from service, use the **no** form of this command.

url-hash {**begin-pattern** | **end-pattern**} *pattern*

no url-hash

Syntax Description

begin-pattern	Specifies the beginning of the URL to parse.
end-pattern	Specifies the ending of the URL to parse.
pattern	Pattern string to parse.

Defaults

URL hashing is off.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The beginning and ending patterns apply to the URL hashing algorithm that is set using the **predictor** command in the SLB server farm submode.

Examples

This example shows how to specify a URL pattern to parse:

```
Cat6k-2(config-slb-vserver)# url hash begin pattern lslkjfsj
```

Related Commands

predictor (serverfarm submode)
show module csm vserver redirect

virtual (virtual server submode)

To configure virtual server attributes, use the **virtual** command in the SLB virtual server configuration submode. To set the virtual server's IP address to 0.0.0.0 and its port number to zero, use the **no** form of this command.

virtual *ip-address* [*ip-mask*] **tcp** *port* [**service** {**ftp** | **rtsp** | **termination**}]

virtual *ip-address* [*ip-mask*] **udp** *port* [**service** {**rtsp** | **per packet**}]

virtual *ip-address* [*ip-mask*] {**any** | *protocol-number*} [**service per-packet**]

no virtual *ip-address*

Syntax Description

ip-address	IP address for the virtual server.
ip-mask	(Optional) Mask for the IP address to allow connections to an entire network.
tcp *port*	Specifies the TCP port.
service ftp	(Optional) Combines connections associated with the same service so that all related connections from the same client use the same real server. FTP data connections are combined with the control session that created them. If you want to configure FTP services, these keywords are required.
service rtsp	(Optional) Combines connections to the Real Time Streaming Protocol (RTSP) TCP port 554.
service termination	(Optional) Enables TCP termination for DoS attack protection.
udp *port*	Specifies the UDP port.
any | *protocol-number*	Load-balancing protocol, either TCP, UDP, any, or a number from 0 to 255.
service per-packet	(Optional) Enables load balancing for each packet independently. This option is for non-TCP only.

Defaults

The default IP mask is 255.255.255.255.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced.
CSM release 2.1(1)	*ip-netmask*, UDP/arbitrary protocol introduced.
CSM release 2.2.1	RTSP support introduced.
CSM release 3.2(1)	Added TCP termination for DoS attack prevention and per packet load balancing.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Clients connecting to the virtual server use this address to access the server farm. A port of 0 (or **any**) means that this virtual server handles all ports not specified for handling by another virtual server with the same IP address. The port is used only for TCP or UDP load balancing. No virtual servers can be configured with the same virtual settings and VLAN.

The following TCP port names can be used in place of a number:

XOT—**X25** over TCP (1998)

dns—Domain Name Service (53)

ftp—File Transfer Protocol (21)

https—HTTP over Secure Sockets Layer (443)

matip-a—Mapping of Airline Traffic over IP, Type A (350)

nntp—Network News Transport Protocol (119)

pop2—Post Office Protocol v2 (109)

pop3—Post Office Protocol v3 (110)

smtp—Simple Mail Transport Protocol (25)

telnet—Telnet (23)

www—World Wide Web—Hypertext Transfer Protocol (80)

any—Traffic for any port (the same as specifying a 0).

The Cisco Content Switching Module allows virtual server configuration with the RTSP service. The implementation supports 4 ports from streams data traffic, and the number of media streams in one RTSP presentation is limited to 2. It is possible to handle the TCP and UDP traffic separately, and link them using sticky. This example (replace IP-x with valid IP address) shows how to separate TCP and UDP traffic:

```
Cat6k-2(config-module-csm)# serverfarm TEST
Cat6k-2(config-slb-sfarm)# nat server
Cat6k-2(config-slb-sfarm)# no nat client
Cat6k-2(config-module-csm)# real IP-1
Cat6k-2(config-slb-real)# inservice
Cat6k-2(config-module-csm)# real IP-2
Cat6k-2(config-slb-real)# inservice
Cat6k-2(config-module-csm)# real IP-3
Cat6k-2(config-slb-real)# inservice
!
Cat6k-2(config-module-csm)# sticky 7 netmask 255.255.255.255 address source timeout 5
!
Cat6k-2(config-module-csm)# vserver RTSP
Cat6k-2(config-slb-vserver)# virtual IP-4 tcp any
Cat6k-2(config-slb-vserver)# serverfarm TEST
Cat6k-2(config-slb-vserver)# sticky 5 group 7
Cat6k-2(config-slb-vserver)# persistent rebalance
Cat6k-2(config-slb-vserver)# inservice
!
Cat6k-2(config-module-csm)# vserver RTSP2
Cat6k-2(config-slb-vserver)# virtual IP-4 udp any
Cat6k-2(config-slb-vserver)# serverfarm TEST
Cat6k-2(config-slb-vserver)# sticky 5 group 7
Cat6k-2(config-slb-vserver)# persistent rebalance
Cat6k-2(config-slb-vserver)# inservice
```

Examples

This example shows how to create a virtual server and assign it an IP address, protocol, and port:

```
Cat6k-2(config-slb-vserver)# virtual 102.35.44.79 tcp 1
```

Related Commands

advertise (virtual server submode)
show module csm vserver

vlan (virtual server submode)

To define which source VLANs may access the virtual server, use the **vlan** command in the SLB virtual server submode. To remove the VLAN, use the **no** form of this command.

vlan *vlan-number* **local**

no vlan

Syntax Description

vlan-number	VLAN that the virtual server may access.
local	Allows the virtual server to accept connections from the SSL daughter card.

Defaults

The default is all VLANs.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The VLAN must correspond to an SLB VLAN previously created with the **vlan** command.

Examples

This example shows how to specify a VLAN for virtual server access:

```
Cat6k-2(config-slb-vserver)# vlan 5
```

Related Commands

show module csm vserver redirect
show module csm vlan
vlan (virtual server submode)

vlan

To define which source VLANs may access the virtual server, and then enter the VLAN submode, use the **vlan** command in the CSM submode. To remove the VLAN, use the **no** form of this command.

vlan *vlan-number* [**client** | **server**]

no vlan

Syntax Description

vlan-number	VLAN that the virtual server may access.
client | **server**	(Optional) Specifies the client-side or server-side VLAN.

Defaults

The default is all VLANs.

Command Modes

SLB configuration submode

Command History

Release	Modification
CSM release 2.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The VLAN must correspond to an SLB VLAN previously created with the **vlan** command.

Examples

This example shows how to specify a VLAN for virtual server access:

```
Cat6k-2(config-slb-csm)# vlan 5
```

Related Commands

alias (VLAN submode)
gateway (VLAN submode)
ip address (VLAN submode)
route (VLAN submode)
show module csm vlan

alias (VLAN submode)

To assign multiple IP addresses to the CSM, use the **alias** command in the SLB VLAN configuration submode.To remove an alias IP addresses from the configuration, use the **no** form of this command.

alias *ip-address netmask*

no alias *ip-address netmask*

Syntax Description

ip-address	Alias IP address; a maximum of 255 addresses are allowed per VLAN.
netmask	Network mask.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced for server VLANs.
CSM release 2.1(1)	This command is now available for both client and server VLANs.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command allows you to place the CSM on a different IP network than real servers without using a router.

If the ICMP protocol does not terminate, you may need to set the idle timeout of these connections. The alias IP address in the CSM serves three purposes:

- It is a shared next hop (gateway) for two CSMs in the redundant configuration. The servers should point to the alias as the default gateway. The Route Health Injection (RHI) service would be using the alias IP address as the next hop when inserting a route.
- If ping is destined to the alias IP address, the CSM sends the reply back to the source MAC. This reply is useful when performing an ICMP probe from one CSM, across a firewall farm, to the other CSM alias address.
- In the Global Server Load Balancing (GSLB) configuration, the alias IP address is the destination VIP for the DNS request.

Examples

This example shows how to assign multiple IP addresses to the CSM:

```
Cat6k-2(config-slb-vlan-server)# alias 130.21.34.56 255.255.255.0
Cat6k-2(config-slb-vlan-server)# alias 130.22.35.57 255.255.255.0
Cat6k-2(config-slb-vlan-server)# alias 130.23.36.58 255.255.255.0
Cat6k-2(config-slb-vlan-server)# alias 130.24.37.59 255.255.255.0
Cat6k-2(config-slb-vlan-server)# alias 130.25.38.60 255.255.255.0
```

Related Commands

show module csm vlan
vlan (XML submode)

description (VLAN submode)

To add a description for the VLAN, use the **description** command in the SLB VLAN configuration submode.To remove the description, use the **no** form of this command.

description *line*

no description

Syntax Description

line	Description text.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 4.2(1)	This command was introduced.

Examples

This example shows how to add a description:

```
Cat6k-2(config-slb-vlan-client)# description Backup Server Farm
```

Related Commands

ip address (VLAN submode) (SLB VLAN configuration submode)
show module csm vlan
vlan (virtual server submode)

gateway (VLAN submode)

To configure a gateway IP address, use the **gateway** command in the SLB VLAN configuration submode .To remove the gateway from the configuration, use the **no** form of this command.

gateway *ip-address*

no gateway *ip-address*

Syntax Description

ip-address	IP address of the client-side gateway.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced for client VLANs.
CSM release 2.1(1)	This command is now available for both client and server VLANs.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can configure up to 7 gateways per VLAN with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the **ip address** SLB VLAN command.

Examples

This example shows how to configure a client-side gateway IP address:

```
Cat6k-2(config-slb-vlan-client)# gateway 130.21.34.56
```

Related Commands

ip address (VLAN submode) (SLB VLAN configuration submode)
show module csm vlan
vlan (virtual server submode)

ip address (VLAN submode)

To assign an IP address to the CSM that is used for probes and ARP requests on a VLAN, use the **ip address** command in the SLB VLAN configuration submode.To remove the CSM IP address and disable probes and ARP requests from the configuration, use the **no** form of this command.

ip address *active_ip_addr netmask* **alt** *standby_ip_addr netmask*

no ip address

Syntax Description

netmask	Network mask.
active_ip_addr	IP address for the active CSM; only one management IP address is allowed per client or server VLAN.
standby_ip_addr	IP address for the standby CSM.
alt	Configures the alternate VLAN IP address.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM-S release 1.1(1)	This command was introduced.
CSM release 2.2.1	Increases maximum number of unique VLAN IP addresses per system form 32 to 255.
CSM-S release 2.1(1)	Adds the **alt** keyword to specify IP address of active and standby CSM for client or server VLAN.

Usage Guidelines

This command is applicable for both server and client VLANs. Up to 255 unique VLAN IP addresses are allowed per module.

Examples

This example shows how to assign an IP address to the CSM:

```
Cat6k-2(config-slb-vlan-client)# ip address 130.21.34.56 255.255.255.0
```

Related Commands

show module csm vlan
vlan (virtual server submode)

route (VLAN submode)

To configure networks that are one Layer 3 hop away from the CSM, use the **route** command in the SLB VLAN configuration submode .To remove the subnet or gateway IP address from the configuration, use the **no** form of this command.

route *ip-address netmask* **gateway** *gw-ip-address*

no route *ip-address netmask* **gateway** *gw-ip-address*

Syntax Description

ip-address	Subnet IP address.
netmask	Network mask.
gateway	Specifies that the gateway is configured.
gw-ip-address	Gateway IP address.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
CSM release 1.1(1)	This command was introduced for server VLANs.
CSM release 2.1(1)	This command is now available for both client and server VLANs.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You specify the Layer 3 networks subnet address and the gateway IP address to reach the next-hop router. The gateway address must be in the same network as specified in the **ip address** SLB VLAN command.

Examples

This example shows how to configure a network to the CSM:

```
Cat6k-2(config-slb-vlan-server)# route 130.21.34.56 255.255.255.0 gateway 120.22.36.40
```

Related Commands

ip address (VLAN submode)
show module csm vlan
vlan (virtual server submode)

xml-config

To enable XML for a CSM module, and then enter the XML configuration submode, use the **xml-config** command. To remove the XML configuration, use the **no** form of this command.

xml-config

no xml-config

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the XML configuration:

```
Cat6k-2(config-module-csm)# xml-config
Cat6k-2(config-slb-xml)#
```

Related Commands

client-group (XML submode)
credentials (XML submode)
vlan (XML submode)

client-group (XML submode)

To allow only connections sourced from an IP address matching the client group, use the **client-group** command in the SLB XML configuration submode. To remove the client group connections, use the **no** form of this command.

client-group [*1–99* | *name*]

no client-group

Syntax Description

1–99	(Optional) Client group number.
name	(Optional) Name of the client group.

Defaults

Client group connections are removed.

Command Modes

SLB XML configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When a client group is specified, only connections sourced from an IP address matching that client group are accepted by the CSM XML configuration interface. If no client group is specified, then no source IP address check is performed. Only one client group may be specified.

Examples

This example shows how to specify a client group:

```
Cat6k-2(config-slb-xml)# client-group domino
```

Related Commands

xml-config

credentials (XML submode)

To define one or more username and password combinations, use the **credentials** command in the SLB XML configuration submode. To remove the credentials, use the **no** form of this command.

credentials *user-name password*

no credentials *user-name*

Syntax Description

user-name	Name of the credentials user.
password	Password for the credentials user.

Defaults

This command has no default settings.

Command Modes

SLB XML configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

When one or more credentials commands are specified, the CSM HTTP server authenticates user access.

Examples

This example shows how to specify the user and password credentials for access:

```
Cat6k-2(config-slb-xml)# credentials savis XXXXX
```

Related Commands

client-group (XML submode)
xml-config

inservice (XML submode)

To enable XML for use by the CSM, use the **inservice** command in the SLB XML configuration submode. If this command is not specified, XML is not used. To disable XML, use the **no** form of this command.

inservice

no inservice

Defaults

This command has no default settings.

Command Modes

SLB XML configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable XML:

```
Cat6k-2(config-slb-xml)# inservice
```

Related Commands

xml-config

port (XML submode)

To specify the TCP port on which the CSM HTTP server listens, use the **port** command in the SLB XML configuration submode. To remove the port, use the **no** form of this command.

port *port-number*

no port

Syntax Description

port-number	Sets the CSM port.

Defaults

The default is port 80.

Command Modes

SLB XML configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify the TCP port for the server:

```
Cat6k-2(config-slb-xml)# port 80
```

Related Commands

client-group (XML submode)

vlan (XML submode)

To restrict the CSM HTTP server to accept connections only from the specified VLAN, use the **vlan** command in the SLB XML configuration submode. To specify that all VLANs are accepted, use the **no** form of this command.

vlan *id*

no vlan

Syntax Description

id	VLAN name.

Defaults

All VLANs are accepted.

Command Modes

SLB XML configuration submode

Command History

Release	Modification
CSM release 3.1(1)	This command was introduced.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to specify an owner for virtual server access:

```
Cat6k-2(config-slb-xml)# vlan 9
```

Related Commands

client-group (XML submode)

CHAPTER 3

Commands Specific to the Content Switching Module with SSL

This chapter contains an alphabetical listing of SSL specific commands for the Catalyst 6500 series switch Content Switching Module with SSL.

These commands are not supported on the Catalyst 6500 series switch Content Switching Module.

For additional SSL services information, refer to the following documentation:

- *Release Notes for the Catalyst 6500 Series Switch Content Switching Module with SSL*
- *Catalyst 6500 Series Content Switching Module with SSL Installation and Configuration Note*

Table 3-1 provides a brief description of the commands contained in this appendix.

Table 3-1 Command Descriptions

Command	Description
clear ssl-proxy conn	Clears the SSL connections.
clear ssl-proxy session	Resets the entries from the session cache.
clear ssl-proxy stats	Resets the statistics counters maintained in different SSL Services Module system components.
crypto ca export pem	Exports privacy-enhanced mail (PEM) files from the SSL Services Module.
crypto ca import pem	Imports a PEM file to the SSL Services Module.
crypto ca export pkcs12	Exports a PKCS12 file from the SSL Services Module.
crypto ca import pkcs12	Imports a PKCS12 file to the SSL Services Module.
crypto key export rsa pem	Exports a PEM-formatted RSA key from the SSL Services Module.
crypto key import rsa pem	Imports a PEM-formatted RSA key to the SSL Services Module.
debug ssl-proxy	Turns on the debug flags in different system components.
show ssl-proxy admin-info	Displays the administration VLAN and related IP and gateway addresses.
show ssl-proxy buffers	Displays the TCP buffer usage information.
show ssl-proxy certificate-history	Displays the certificate event history information.

Table 3-1 Command Descriptions (continued)

Command	Description
show ssl-proxy conn	Displays the TCP connections from the SSL Services Module.
show ssl-proxy crash-info	Displays the crash information.
show ssl-proxy mac address	Displays the current MAC address.
show ssl-proxy natpool	Displays NAT pool information.
show ssl-proxy policy	Displays the configured SSL or TCP policies.
show ssl-proxy service	Displays the configured SSL virtual server information.
show ssl-proxy stats	Displays statistics counter information.
show ssl-proxy status	Displays status information.
show ssl-proxy version	Displays the current image version.
show ssl-proxy vlan	Displays VLAN information.
show ssl-proxy vts	Displays VTS information.
show ssl-proxy vts	Configures the SNMP traps and informs.
ssl-proxy crypto selftest	Initiates a cryptographic self-test.
ssl-proxy mac address	Configures a MAC address.
ssl-proxy natpool	Defines a pool of IP addresses that the SSL module uses for implementing the client NAT.
ssl-proxy pki	Configure and defines the PKI implementation on SSL service module.
ssl-proxy policy http-header	Enters the HTTP header configuration submode where you can define the HTTP header insertion content policy applied to the payload.
ssl-proxy policy ssl	Enters the SSL-policy configuration submode where you can define the SSL of a TCP policy for one or more SSL proxy services.
ssl-proxy policy tcp	Enters the proxy-policy TCP configuration submode where you can define the TCP policy templates.
ssl-proxy policy url-rewrite	Enters the URL rewrite configuration submode where you can define the URL rewrite content policy applied to the payload.
ssl-proxy pool ca	Enters the certificate authority pool configuration submode where you can configure a list of certificate agents (CAs) that the module can trust into a pool.
ssl-proxy service	Enters the proxy-service configuration submode where you can configure the virtual IP address and port associated with the proxy service and the associated target IP address and port. You can also define TCP and SSL policies for both the client side and the server side of the proxy.
ssl-proxy ssl ratelimit	Prohibits new connections during overload conditions.
ssl-proxy vlan	Enters the proxy VLAN configuration submode where you can configure a VLAN for the SSL Services Module.

Table 3-2 lists the modes and submode commands.

Table 3-2 Commands and Submode Commands

Commands	Submode Commands
ssl-proxy pki	[**no**] **authenticate** {**timeout** *seconds*}
	[**no**] **cache** {{**size** *entries*} | {**timeout** *minutes*}}
	[**no**] **certificate {check-expiring** {**interval** *hours*}}
	[**no**] **history**
ssl-proxy policy http-header	**client-cert**
	client-ip-port
	custom *custom-string*
	prefix
	session
ssl-proxy policy ssl	**cipher** {**rsa-with-3des-ede-cbc-sha** | **rsa-with-des-cbc-sha** | **rsa-with-rc4-128-md5** | **rsa-with-rc4-128-sha** | **all**}
	[**no**] **close-protocol**
	default {**cipher** | **close-protocol** | **session-cache** | **version**}
	exit
	help
	[**no**] **session-cache**
	[**no**] **session-cache size** *size*
	[**no**] **timeout handshake** *time*
	[**no**] **timeout session** *time* [**absolute**]
	version {**all** | **ssl3** | **tls1**}
ssl-proxy policy tcp	**exit**
	help
	[**no**] **buffer-share rx** *buffer-limit-in-bytes*
	[**no**] **buffer-share tx** *buffer-limit-in-bytes*
	[**no**] **timeout inactivity** *timeout-in-seconds*
	[**no**] **mss** *max-segment-size-in-bytes*
	[**no**] **timeout fin-wait** *timeout-in-seconds*
	[**no**] **timeout reassembly** *time-in-seconds*
	[**no**] **timeout syn** *timeout-in-seconds*
ssl-proxy policy url-rewrite	*hostname*
	clearport *port-number*
	sslport *port-number*

Table 3-2 Commands and Submode Commands (continued)

Commands	Submode Commands
ssl-proxy service	**certificate rsa general-purpose trustpoint** *trustpoint-name*
	default {**nat**}
	exit
	help
	inservice
	nat {**server** | **client** *natpool-name*}
	server ipaddr *ip-addr* **protocol** *protocol* **port** *portno*
	server policy tcp *server-side-tcp-policy-name*
	virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]
	virtual {**policy ssl** *ssl-policy-name*}
	virtual {**policy tcp** *client-side-tcp-policy-name*}
ssl-proxy vlan	**admin**
	exit
	gateway *prefix* [**drop** | **forward**]
	help
	ipaddr *prefix mask*
	no
	route {*prefix mask*} {**gateway** *prefix*}
	standby [*group-number*] {**authentication text** *string*} | {**delay minimum** [*min-delay*] **reload** [*reload-delay*]} | {**ip** [*ip-address* [**secondary**]]} | {**mac-address** *mac-address*} | {**mac-refresh** *seconds*} | {**name** *group-name*} | {**preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]} | {**priority** *priority*} | {**redirects** [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]} | {**timers** [**msec**] *hellotime* [**msec**] *holdtime*} | {**track** *object-number* [**decrement** *priority*]}

clear ssl-proxy conn

To clear all TCP connections on the entire system, use the **clear ssl-proxy conn** command.

clear ssl-proxy conn [**service** *name*]

Syntax Description

service *name*	(Optional) Clears the connections for the specified service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

To reset all the statistics counters that the Content Switching Module with SSL maintains, use the **clear ssl-proxy connection** command without options.

Examples

This example shows how to clear the connections for the specified service:

```
ssl-proxy# clear ssl-proxy conn service S6
```

This example shows how to clear all TCP connections on the entire system:

```
ssl-proxy# clear ssl-proxy conn
ssl-proxy#
```

clear ssl-proxy session

To clear all entries from the session cache, use the **clear ssl-proxy session** command.

clear ssl-proxy session [**service** *name*]

Syntax Description

service *name*	(Optional) Clears the session cache for the specified service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

To clear all entries from the session cache for all services, use the **clear ssl-proxy session** command without options.

Examples

This example shows how to clear the entries from the session cache for the specified service on the Content Switching Module with SSL:

```
ssl-proxy# clear ssl-proxy session service S6
```

This example shows how to clear all entries in the session cache that are maintained on the Content Switching Module with SSL:

```
ssl-proxy# clear ssl-proxy session
ssl-proxy#
```

clear ssl-proxy stats

To reset the statistics counters that are maintained in the different system components on the Content Switching Module with SSL, use the **clear ssl-proxy stats** command.

clear ssl-proxy stats [**crypto** | **fdu** | **ipc** | **pki** | **service** | **ssl** | **tcp**]

Syntax Description

crypto	(Optional) Clears statistics information about the crypto.
fdu	(Optional) Clears statistics information about the F6DU.
ipc	(Optional) Clears statistics information about the inter-process communications (IPC).
pki	(Optional) Clears information about the public key infrastruture (PKI).
service *name*	(Optional) Clears statistics information for a specific service.
ssl	(Optional) Clears statistics information about the SSL.
tcp	(Optional) Clears statistics information about the TCP.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

To reset all the statistics counters that the Content Switching Module with SSL maintains, use the **clear ssl-proxy stats** command without options.

Examples

This example shows how to reset the statistics counters that are maintained in the different system components on the Content Switching Module with SSL:

```
ssl-proxy# clear ssl-proxy stats crypto
ssl-proxy# clear ssl-proxy stats ipc
ssl-proxy# clear ssl-proxy stats pki
ssl-proxy# clear ssl-proxy stats service S6
```

This example shows how to clear all the statistic counters that the Content Switching Module with SSL maintains:

```
ssl-proxy# clear ssl-proxy stats
ssl-proxy#
```

crypto ca export pem

To export privacy-enhanced mail (PEM) files from the Content Switching Module with SSL, use the **crypto ca export pem** command.

crypto ca export *trustpoint_label* **pem** {**terminal** {**des** | **3des**} {**url** *url*}} *pass_phrase*

Syntax Description

trustpoint-label	Name of the trustpoint.
terminal	Displays the request on the terminal.
des	Specifies the 56-bit DES-CBC encryption algorithm.
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the NULL: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
pass_phrase	Pass phrase that is used to protect the private key.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *pass_phrase* value can be any phrase including spaces and punctuation except for a question mark, which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

A key that is marked as unexportable cannot be exported.

You can change the default file extensions when prompted. The default file extensions are as follows:

- public key (.pub)
- private key (.prv)
- certificate (.crt)
- CA certificate (.ca)
- signature key (-sign)
- encryption key (-encr)

Note In SSL software release 1.2, only the private key (.prv), the server certificate (.crt), and the issuer CA certificate (.ca) of the server certificate are exported. To export the whole certificate chain, including all the CA certificates, use a PKCS12 file instead of PEM files.

Examples

This example shows how to export a PEM-formatted file on the Content Switching Module with SSL:

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

crypto ca import pem

crypto ca import pem

To import a PEM-formatted file to the Content Switching Module with SSL, use the **crypto ca import pem** command.

crypto ca import *trustpoint_label* **pem** [**exportable**] {**terminal** | **url** *url* | **usage-keys**} *pass_phrase*

Syntax Description

trustpoint-label	Name of the trustpoint.
exportable	(Optional) Specifies the key that can be exported.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the null: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
pass_phrase	Pass phrase.
usage-keys	Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You will receive an error if you enter the pass phrase incorrectly. The *pass_phrase* value can be any phrase including spaces and punctuation except for a question mark, which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

When importing RSA keys, you can use a public key or its corresponding certificate.

The **crypto ca import pem** command imports only the private key (.prv), the server certificate (.crt), and the issuer CA certificate (.ca). If you have more than one level of CA in the certificate chain, you need to import the root and subordinate CA certificates before this command is issued for authentication. Use cut-and-paste or TFTP to import the root and subordinate CA certificates.

Examples

This example shows how to import a PEM-formatted file from the Content Switching Module with SSL:

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

crypto ca export pem

crypto ca export pkcs12

To export a PKCS12 file from the Content Switching Module with SSL, use the **crypto ca export pkcs12** command.

crypto ca export *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are **scp:, ftp:**, **nvram:**, **rcp:**, and **tftp:**
pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Imported key pairs cannot be exported.

If you are using SSH, we recommend using SCP (secure file transfer) when exporting a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA, and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to export a PKCS12 file using SCP:

```
ssl-proxy(config)# crypto ca export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:
```

```
Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
ssl-proxy(config)#
```

crypto ca import pkcs12

To import a PKCS12 file to the Content Switching Module with SSL, use the **crypto ca import** command.

crypto ca import *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are as follows: • **ftp:**—Imports from the FTP: file system • **nvram:**—Imports from the NVRAM: file system • **rcp:**—Imports from the RCP: file system • **scp:**—Imports from the SCP: file system • **tftp:**—Imports from the TFTP: file system
pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Command Modes

If you are using SSH, we recommend using SCP (secure file transfer) when importing a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or to enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to import a PKCS12 file using SCP:

```
ssl-proxy(config)# crypto ca import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
ssl-proxy(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
ssl-proxy(config)#
```

crypto key export rsa pem

To export a PEM-formatted RSA key to the Content Switching Module with SSL, use the **crypto key export rsa pem** command.

crypto key export rsa *keylabel* **pem** {**terminal** | **url** *url*} {{**3des** | **des**} [**exportable**] *pass_phrase*}

Syntax Description

keylabel	Name of the key.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the null: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
des	Specifies the 56-bit DES-CBC encryption algorithm.
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
exportable	(Optional) Specifies that the key can be exported.
pass_phrase	Pass phrase.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for a question mark, which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to export a key from the Content Switching Module with SSL:

```
ssl-proxy(config)# crypto key export rsa test-keys pem url scp: 3des password
% Key name:test-keys
   Usage:General Purpose Key
Exporting public key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.pub]?

Password:

Writing test-keys.pub Writing file to scp://lab@7.0.0.7/test-keys.pub
Password:
!
Exporting private key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.prv]?

Password:

Writing test-keys.prv Writing file to scp://lab@7.0.0.7/test-keys.prv
Password:
ssl-proxy(config)#
```

crypto key import rsa pem

To import a PEM-formatted RSA key from an external system, use the **crypto key import rsa pem** command.

crypto key import rsa *keylabel* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*}

Syntax Description

keylabel	Name of the key.
usage-keys	(Optional) Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Imports from the FTP: file system • **null:**—Imports from the null: file system • **nvram:**—Imports from the NVRAM: file system • **rcp:**—Imports from the RCP: file system • **scp:**—Imports from the SCP: file system • **system:**—Imports from the system: file system • **tftp:**—Imports from the TFTP: file system
exportable	(Optional) Specifies that the key can be exported.
passphrase	Pass phrase.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for a question mark, which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to import a PEM-formatted RSA key from an external system and export the PEM-formatted RSA key to the Content Switching Module with SSL:

```
ssl-proxy(config)# crypto key import rsa newkeys pem url scp: password
% Importing public key or certificate PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.pub]? test-keys.pub

Password:
Sending file modes:C0644 272 test-keys.pub
Reading file from scp://lab@7.0.0.7/test-keys.pub!
% Importing private key PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.prv]? test-keys.prv

Password:
Sending file modes:C0644 963 test-keys.prv
Reading file from scp://lab@7.0.0.7/test-keys.prv!% Key pair import succeeded.

ssl-proxy(config)#
```

debug ssl-proxy

To turn on the debug flags in different system components, use the **debug ssl-proxy** command. Use the **no** form of this command to turn off the debug flags.

debug ssl-proxy {**app** | **fdu** [*type*] | **ipc** | **pki** [*type*] | **ssl** [*type*] | **tcp** [*type*]}

Syntax Description

app	Turns on App debugging.
fdu *type*	Turns on FDU debugging; (optional) *type* valid values are **cli**, **hash**, **ipc**, and **trace**. See the “Usage Guidelines” section for additional information.
ipc	Turns on IPC debugging.
pki *type*	Turns on PKI debugging; (optional) *type* valid values are **cert**, **events**, **history**, **ipc**, and **key**. See the “Usage Guidelines” section for additional information.
ssl *type*	Turns on SSL debugging; (optional) *type* valid values are **alert**, **error**, **handshake**, and **pkt**. See the “Usage Guidelines” section for additional information.
tcp *type*	Turns on TCP debugging; (optional) *type* valid values are **event**, **packet**, **state**, and **timers**. See the “Usage Guidelines” section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The **fdu** *type* includes the following values:

- **cli**—Debugs the FDU CLI.
- **hash**—Debugs the FDU hash.
- **ipc** —Debugs the FDU IPC.
- **trace**—Debugs the FDU trace.

The **pki** *type* includes the following values:

- **certs**—Debugs the certificate management.
- **events**—Debugs events.
- **history**—Debugs the certificate history.
- **ipc**—Debugs the IPC messages and buffers.
- **key**—Debugs key management.

The **ssl** *type* includes the following values:

- **alert**—Debugs the SSL alert events.
- **error**—Debugs the SSL error events.
- **handshake**—Debugs the SSL handshake events.
- **pkt**—Debugs the received and transmitted SSL packets.

Note Use the TCP debug commands only to troubleshoot basic connectivity issues under little or no load conditions (for instance, when no connection is being established to the virtual server or real server).

If you run TCP debug commands, the TCP module displays large amounts of debug information on the console, which can significantly slow down module performance. Slow module performance can lead to delayed processing of TCP connection timers, packets, and state transitions.

The **tcp** *type* includes the following values:

- **events**—Debugs the TCP events.
- **pkt**—Debugs the received and transmitted TCP packets.
- **state**—Debugs the TCP states.
- **timers**—Debugs the TCP timers.

Examples

This example shows how to turn on App debugging:

```
ssl-proxy# debug ssl-proxy app
ssl-proxy#
```

This example shows how to turn on FDU debugging:

```
ssl-proxy# debug ssl-proxy fdu
ssl-proxy#
```

This example shows how to turn on IPC debugging:

```
ssl-proxy# debug ssl-proxy ipc
ssl-proxy#
```

This example shows how to turn on PKI debugging:

```
ssl-proxy# debug ssl-proxy pki
ssl-proxy#
```

This example shows how to turn on SSL debugging:

```
ssl-proxy# debug ssl-proxy ssl
ssl-proxy#
```

This example shows how to turn on TCP debugging:

```
ssl-proxy# debug ssl-proxy tcp
ssl-proxy#
```

This example shows how to turn off TCP debugging:

```
ssl-proxy# no debug ssl-proxy tcp
ssl-proxy#
```

do

To execute EXEC-level commands from global configuration mode or other configuration modes or submodes, use the **do** command.

do *command*

Syntax Description

command	EXEC-level command to be executed.

Defaults

This command has no default settings.

Command Modes

Global configuration or any other configuration mode or submode from which you are executing the EXEC-level command.

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Caution Do not enter the **do** command in EXEC mode. Interruption of service may occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the mode to configuration mode.

You cannot use the **do** command to execute the **copy** or **write** command in the global configuration or any other configuration mode or submode.

Examples

This example shows how to execute the EXEC-level **show interfaces** command from within global configuration mode:

```
ssl-proxy(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
ssl-proxy(config)#
```

show ssl-proxy admin-info

To display the administration VLAN and related IP and gateway addresses, use the **show ssl-proxy admin-info** command.

show ssl-proxy admin-info

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the administration VLAN and related IP and gateway addresses:

```
ssl-proxy# show ssl-proxy admin-info
STE administration VLAN: 2
STE administration IP address: 207.57.100.18
STE administration gateway: 207.0.207.5
ssl-proxy#
```

Related Commands

ssl-proxy vlan

show ssl-proxy buffers

To display information about TCP buffer usage, use the **show ssl-proxy buffers** command.

show ssl-proxy buffers

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the buffer usage and other information in the TCP subsystem:

```
ssl-proxy# show ssl-proxy buffers
Buffers info for TCP module 1
TCP data buffers used 2816 limit 112640
TCP ingress buffer pool size 56320 egress buffer pool size 56320
TCP ingress data buffers min-thresh 7208960 max-thresh 21626880
TCP ingress data buffers used Current 0 Max 0
TCP ingress buffer RED shift 9 max drop prob 10
Conns consuming ingress data buffers 0
Buffers with App 0
TCP egress data buffers used Current 0 Max 0
Conns consuming egress data buffers 0
In-sequence queue bufs 0 OOO bufs 0
ssl-proxy#
```

Related Commands

ssl-proxy policy tcp

show ssl-proxy certificate-history

To display information about the event history of the certificate, use the **show ssl-proxy certificate-history** command.

show ssl-proxy certificate-history [**service** [*name*]]

Syntax Description

service *name*	(Optional) Displays all certificate records of a proxy service and (optionally) for a specific proxy service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The **show ssl-proxy certificate-history** command displays these records:

- Service name
- Key pair name
- Generation or import time
- Trustpoint name
- Certificate subject name
- Certificate issuer name
- Serial number
- Date

A syslog message is generated for each record. The oldest records are deleted after the limit of 512 records is reached.

Examples

This example shows how to display the event history of all the certificate processing:

```
ssl-proxy# show ssl-proxy certificate-history
Record 1, Timestamp:00:00:51, 16:36:34 UTC Oct 31 2002
    Installed Server Certificate, Index 5
    Proxy Service:s1,  Trust Point:t3
    Key Pair Name:k3,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:12:27:58 UTC Oct 30 2002
    Subject Name:OID.1.2.840.113549.1.9.2 = simpson5-2-ste.cisco.com,
OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5D3D1931000100000D99
    Validity Start Time:21:58:12 UTC Oct 30 2002
    End Time:22:08:12 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 2, Timestamp:00:01:06, 16:36:49 UTC Oct 31 2002
    Installed Server Certificate, Index 6
    Proxy Service:s5,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
% Total number of certificate history records displayed = 4
ssl-proxy#
```

This example shows how to display the certificate record for a specific proxy service:

```
ssl-proxy# show ssl-proxy certificate-history service s6
Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
Total number of certificate history records displayed = 2
```

Related Commands

ssl-proxy service

show ssl-proxy conn

To display the TCP connections from the Content Switching Module with SSL, use the **show ssl-proxy conn** command.

show ssl-proxy conn 4tuple [**local** {**ip** *local-ip-addr local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**port** *local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]

show ssl-proxy conn service *name*

Syntax Description

4tuple	Displays the TCP connections for a specific address.
local	(Optional) Displays the TCP connections for a specific local device.
ip *local-ip-addr*	(Optional) IP address of a local device.
local-port	(Optional) Port number of a local device.
remote	(Optional) Displays the TCP connections for a specific remote device.
ip *remote-ip-addr*	(Optional) IP address of a remote device.
port *remote-port*	(Optional) Port number of a remote device.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

These examples show different ways to display the TCP connection that is established from the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy conn
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.0.0.10:4430         1.200.200.14:48582    2    0      0      0      ESTAB
1.200.200.14:48582    2.100.100.72:80       2    1      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48583    2    2      0      0      ESTAB
1.200.200.14:48583    2.100.100.72:80       2    3      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48584    2    4      0      0      ESTAB
1.200.200.14:48584    2.100.100.72:80       2    5      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48585    2    6      0      0      ESTAB
1.200.200.14:48585    2.100.100.72:80       2    7      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48586    2    8      0      0      ESTAB
1.200.200.14:48586    2.100.100.72:80       2    9      0      0      ESTAB

ssl-proxy# show ssl-proxy conn 4tuple local port 443
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.133:443       1.200.200.12:39728    2    113676 0      0      TWAIT
No Bound Connection

2.50.50.133:443       1.200.200.12:39729    2    113680 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:40599    2    113684 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48031    2    114046 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48032    2    114048 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48034    2    114092 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48035    2    114100 0      0      TWAIT
No Bound Connection
```

```
ssl-proxy# show ssl-proxy conn 4tuple remote ip 1.200.200.14
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:38814    2    58796  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38815    2    58800  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38817    2    58802  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38818    2    58806  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38819    2    58810  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38820    2    58814  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38821    2    58818  0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn service iis1
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:41217    2    121718 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41218    2    121722 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41219    2    121726 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41220    2    121794 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41221    2    121808 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41222    2    121940 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41223    2    122048 0      0      TWAIT
No Bound Connection
```

show ssl-proxy crash-info

To collect information about the software-forced reset from the Content Switching Module with SSL, use the **show ssl-proxy crash-info** command.

show ssl-proxy crash-info [**brief** | **details**]

Syntax Description

brief	(Optional) Collects a small subset of software-forced reset information, limited to processor registers.
details	(Optional) Collects the full set of software-forced reset information, including exception and interrupt stacks dump (this can take up to 10 minutes to complete printing).

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to collect information about the software-forced reset:

```
ssl-proxy# show ssl-proxy crash-info

===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

NVRAM CHKSUM:0xEB28
NVRAM MAGIC:0xC8A514F0
NVRAM VERSION:1

++++++++++ CORE 0 (FDU) ++++++++++++++++++++++

   CID:0
   APPLICATION VERSION:2003.04.15 14:50:20 built for cantuc
   APPROXIMATE TIME WHEN CRASH HAPPENED:14:06:04 UTC Apr 16 2003
   THIS CORE DIDN'T CRASH
   TRACEBACK:222D48 216894
   CPU CONTEXT  -----------------------------

$0 :00000000, AT :00240008, v0 :5A27E637, v1 :000F2BB1
a0 :00000001, a1 :0000003C, a2 :002331B0, a3 :00000000
```

```
t0 :00247834, t1 :02BFAAA0, t2 :02BF8BB0, t3 :02BF8BA0
t4 :02BF8BB0, t5 :00247834, t6 :00000000, t7 :00000001
s0 :00000000, s1 :0024783C, s2 :00000000, s3 :00000000
s4 :00000001, s5 :0000003C, s6 :00000019, s7 :0000000F
t8 :00000001, t9 :00000001, k0 :00400001, k1 :00000000
gp :0023AE80, sp :031FFF58, s8 :00000019, ra :00216894
LO :00000000, HI :0000000A, BADVADDR :828D641C
EPC :00222D48, ErrorEPC :BFC02308, SREG :34007E03
Cause 0000C000 (Code 0x0):Interrupt exception

CACHE ERROR registers  -------------------

CacheErrI:00000000, CacheErrD:00000000
ErrCtl:00000000, CacheErrDPA:0000000000000000

   PROCESS STACK -----------------------------
      stack top:0x3200000

   Process stack in use:

   sp is close to stack top;

   printing 1024 bytes from stack top:

031FFC00:06405DE0 002706E0 0000002D 00000001  .@]`.'.`...-....
031FFC10:06405DE0 002706E0 00000001 0020B800  .@]`.'.`..... 8.
031FFC20:031FFC30 8FBF005C 14620010 24020004  ..|0.?.\.b..$...
...........
...........
...........
FFFFFFD0:00000000 00000000 00000000 00000000 ................
FFFFFFE0:00627E34 00000000 00000000 00000000 .b~4............
FFFFFFF0:00000000 00000000 00000000 00000006 ................


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

This example shows how to collect a small subset of software-forced reset information:

```
ssl-proxy# show ssl-proxy crash-info brief


===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

SKE CRASH INFO Error: wrong MAGIC # 0

CLI detected an error in FDU_IOS crash-info; wrong magic.

------------- COMPLEX 1 [TCP_SSL] ----------------------


Crashinfo fragment #0 from core 2 at offset 0 error:
Remote system reports wrong crashinfo magic.
Bad fragment received. Reception abort.

CLI detected an error in TCP_SSL crash-info;


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

show ssl-proxy mac address

To display the current MAC address, use the **show ssl-proxy mac address** command.

show ssl-proxy mac address

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the current MAC address that is used in the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy mac address
STE MAC address: 00e0.b0ff.f232
ssl-proxy#
```

show ssl-proxy natpool

To display information about the NAT pool, use the **show ssl-proxy natpool** command.

show ssl-proxy natpool [*name*]

Syntax Description

name	(Optional) NAT pool name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display information for a specific NAT address pool that is configured on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy natpool NP1
Start ip: 207.57.110.1
End ip: 207.57.110.8
netmask: 255.0.0.0
vlan associated with natpool: 2
SSL proxy services using this natpool:
S2
S3
S1
S6
Num of proxies using this natpool: 4
ssl-proxy#
```

Related Commands

ssl-proxy natpool

show ssl-proxy policy

To display the configured SSL proxy policies, use the **show ssl-proxy policy** command.

show ssl-proxy policy {**http-header** | **ssl** | **tcp** | **url-rewrite**} [*name*]

Syntax Description

http-header	Displays the configured HTTP header policies.
ssl	Displays the configured SSL policies.
tcp	Displays the configured TCP policies.
url-rewrite	Displays the configured URL rewrite policies.
name	(Optional) Policy name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the **http-header** and **url-rewrite** keywords.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display information about the HTTP header policy:

```
ssl-proxy# show ssl-proxy policy http-header httphdr-policy
 Client Certificate Insertion Header Only
 Session Header Insertion All
 Client IP/Port Insertion Client IP and Port
 Hdr # Custom Header
   0 SSL-Frontend:Enable

>Usage count of this policy: 0
ssl-proxy#
```

This example shows how to display policy information about a specific SSL policy that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy ssl ssl-policy1
Cipher suites: (None configured, default ciphers included)
        rsa-with-rc4-128-md5
        rsa-with-rc4-128-sha
        rsa-with-des-cbc-sha
        rsa-with-3des-ede-cbc-sha
```

```
SSL Versions enabled:SSL3.0, TLS1.0
strict close protocol:disabled
Session Cache:enabled
Handshake timeout not configured (never times out)
Num of proxies using this poilicy:0
```

This example shows how to display policy information about a specific TCP policy that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy tcp tcp-policy1
 MSS                  1250
 SYN timeout          75
 Idle timeout          600
 FIN wait timeout     75
 Rx Buffer Share  32768
 Tx Buffer Share  32768

 Usage count of this policy:0
ssl-proxy#
```

This example shows how to display information about the URL rewrite policy:

```
ssl-proxy# show ssl-proxy policy url-rewrite urlrw-policy
 >Rule URL Clearport SSLport
  1 wwwin.cisco.com 80 443
  2 www.cisco.com 8080 444
>
>Usage count of this policy: 0
ssl-proxy#
```

Related Commands

ssl-proxy policy http-header
ssl-proxy policy ssl
ssl-proxy policy tcp
ssl-proxy policy url-rewrite

show ssl-proxy service

To display information about the configured SSL virtual service, use the **show ssl-proxy service** command.

show ssl-proxy service [*name*]

Syntax Description

name	(Optional) Service name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display all SSL virtual services that are configured on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy service
Proxy Service Name Admin Operation Events
status status
S2 up up
S3 up up
S1 up up
S6 down down
ssl-proxy#
```

This example shows how to display a specific SSL virtual service that is configured on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy service S6
Service id: 0, bound_service_id: 256
Virtual IP: 10.10.1.104, port: 443
Server IP: 10.10.1.100, port: 80
Virtual SSL Policy: SSL1_PLC
rsa-general-purpose certificate trustpoint: tptest
  Certificate chain for new connections:
    Server Certificate:
       Key Label: tptest
       Serial Number: 01
    Root CA Certificate:
       Serial Number: 00
  Certificate chain complete
Admin Status: up
Operation Status: down
```

```
Proxy status: No Client VLAN, No Server VLAN
ssl-proxy#
```

show ssl-proxy stats

To display information about the statistics counter, use the **show ssl-proxy stats** command.

show ssl-proxy stats [*type*]

Syntax Description

type	(Optional) Information type; valid values are **crypto**, **ipc**, **pki**, **service**, **ssl**, **fdu** and **tcp**. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	The output of the **show ssl-proxy stats** command was changed to include information about the session allocation failure and session limit-exceed table.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *type* values are defined as follows:

- **crypto**—Displays crypto statistics.
- **ipc**—Displays IPC statistics.
- **pki**—Displays PKI statistics.
- **service**—Displays proxy service statistics.
- **ssl**—Displays SSL detailed statistics.
- **fdu**—Displays FDU processor statistics.
- **tcp**—Displays TCP detailed statistics.

Examples

This example shows how to display all the statistics counters that are collected on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy stats
TCP Statistics:
    Conns initiated     : 20636         Conns accepted      : 20636
    Conns established   : 28744         Conns dropped       : 28744
    Conns closed        : 41272         SYN timeouts        : 0
    Idle timeouts       : 0             Total pkts sent     : 57488
    Data packets sent   : 0             Data bytes sent     : 0
    Total Pkts rcvd     : 70016         Pkts rcvd in seq    : 0
    Bytes rcvd in seq   : 0

SSL Statistics:
    conns attempted     : 20636         conns completed     : 20636
    full handshakes     : 0             resumed handshakes  : 0
    active conns        : 0             active sessions     : 0
    renegs attempted    : 0             conns in reneg      : 0
    handshake failures  : 20636         data failures       : 0
    fatal alerts rcvd   : 0             fatal alerts sent   : 0
    no-cipher alerts    : 0             ver mismatch alerts : 0
    no-compress alerts  : 0             bad macs received   : 0
    pad errors          : 0             session fails       : 0

FDU Statistics:
    IP Frag Drops       : 0             Serv_Id Drops       : 9
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             Checksum Drops      : 0
    IOS Congest Drops   : 0             IP Version Drops    : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 41272         Flow Deletes        : 41272
    conn_id allocs      : 41272         conn_id deallocs    : 41272
    Tagged Drops        : 0             Non-Tagged Drops    : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 3             Enable ipcs         : 0
    Unsolicited ipcs    : 0             Duplicate ADD ipcs  : 0
    IOS broadcast pkts  : 29433         IOS unicast pkts    : 5
    IOS total pkts      : 29438
ssl-proxy#
```

This example shows how to display the PKI statistics:

```
ssl-proxy# show ssl-proxy stats pki
PKI Memory Usage Counters:
  Malloc count: 0
  Setstring count: 0
  Free count: 0
  Malloc failed: 0
  Ipc alloc count: 0
  Ipc free count: 0
  Ipc alloc failed: 0
PKI IPC Counters:
  Request buffer sent: 0
  Request buffer received: 0
  Request duplicated: 0
  Response buffer sent: 0
  Response buffer received: 0
  Response timeout: 0
  Response with error status: 0
  Response with no request: 0
  Response duplicated: 0
  Message type error: 0
PKI Accumulative Certificate Counters:
  Proxy service trustpoint added: 0
  Proxy service trustpoint deleted: 0
  Proxy service trustpoint modified: 0
  Keypair added: 0
  Keypair deleted: 0
  Wrong key type: 0
  Server certificate added: 0
  Server certificate deleted: 0
  Server certificate rolled over: 0
  Server certificate completed: 0
  Intermediate CA certificate added: 0
  Intermediate CA certificate deleted: 0
  Root CA certificate added: 0
  Root CA certificate deleted: 0
  Certificate overwritten: 0
  History records written: 0
  History records read from NVRAM: 0
  Key cert table entries in use: 0
ssl-proxy#
```

This example shows how to display the FDU statistics:

```
ssl-proxy# show ssl-prox stats fdu
FDU Statistics:
    IP Frag Drops       : 0             IP Version Drops    : 0
    IP Addr Discards    : 0             Serv_Id Drops       : 0
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             TCP Checksum Drops  : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 536701        Flow Deletes        : 536701
    Conn Id allocs      : 268354        Conn Id deallocs    : 268354
    Tagged Pkts Drops   : 0             Non-Tagg Pkts Drops : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 1             Enable ipcs         : 0
    Unsolicited ipcs    : 1345          Duplicate Add ipcs  : 0
    IOS Broadcast Pkts  : 43432         IOS Unicast Pkts    : 12899
    IOS Multicast Pkts  : 0             IOS Total Pkts      : 56331
    IOS Congest Drops   : 0             SYN Discards        : 0
FDU Debug Counters:
    Inv. Conn Drops     : 0             Inv. Conn Pkt Drops : 0
    Inv. TCP opcodes    : 0
    Inv. Fmt Pkt Drops  : 0             Inv. Bad Vlan ID    : 0
    Inv. Bad Ctl Command: 0             Inv. TCP Congest    : 0
    Inv. Bad Buffer Fmt : 0             Inv. Buf Undersized : 0
ssl-proxy#
```

show ssl-proxy status

To display information about the Content Switching Module with SSL proxy status, use the **show ssl-proxy status** command.

show ssl-proxy status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	The output of the **show ssl-proxy status** command was changed to include statistics that are displayed at a 1-second, 1-minute, and 5-minute traffic rate for CPU utilization.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the status of the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy status
FDU cpu is alive!
FDU cpu utilization:
    % process util   : 0            % interrupt util : 0

    proc cycles : 0x4D52D1B7        int cycles  : 0x6B6C9937
    total cycles: 0xB954D5BEB6FA
    % process util (5 sec)   : 0            % interrupt util (5 sec) : 0

    % process util (1 min)  : 0            % interrupt util (1 min): 0
    % process util (5 min)  : 0            % interrupt util (5 min) : 0


TCP cpu is alive!
TCP cpu utilization:
    % process util   : 0            % interrupt util : 0

    proc cycles : 0xA973D74D        int cycles  : 0xAA03E1D89A
    total cycles: 0xB958C8FF0E73
    % process util (5 sec)   : 0            % interrupt util (5 sec) : 0

    % process util (1 min)  : 0            % interrupt util (1 min): 0
    % process util (5 min)  : 0            % interrupt util (5 min) : 0
```

```
SSL cpu is alive!
SSL cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0xD475444          int cycles  : 0x21865088E
    total cycles: 0xB958CCEB8059
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0
```

show ssl-proxy version

To display the current image version, use the **show ssl-proxy version** command.

show ssl-proxy version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display the image version that is currently running on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SSL(0.19)  INTERIM TEST
SOFTWARE
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 10-Apr-03 03:03 by integ
Image text-base: 0x00400078, data-base: 0x00ABE000

ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE

ssl-proxy uptime is 3 days, 22 hours, 22 minutes
System returned to ROM by power-on
System image file is "tftp://10.1.1.1/unknown"
AP Version 1.2(1)

ssl-proxy#
```

show ssl-proxy vlan

To display VLAN information, use the **show ssl-proxy vlan** command.

show ssl-proxy vlan [*vlan-id* | **debug**]

Syntax Description

vlan-id	(Optional) VLAN ID. Displays information for a specific VLAN; valid values are from 1 to 1005.
debug	(Optional) Displays debug information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to display all the VLANs that are configured on the Content Switching Module with SSL:

```
ssl-proxy# show ssl-proxy vlan
VLAN index 2 (admin VLAN)
   IP addr 10.1.1.1 NetMask 255.0.0.0 Gateway 10.1.1.5
   Network 10.1.1.2 Mask 255.0.0.0 Gateway 10.1.1.6
VLAN index 3
   IP addr 10.1.1.3 NetMask 255.0.0.0 Gateway 10.1.1.6
VLAN index 6
   IP addr 10.1.1.4 NetMask 255.0.0.0

ssl-proxy#
```

Related Commands

ssl-proxy vlan

show ssl-proxy vts

To display SSL proxy VLAN information, use the **show ssl-proxy vlan** command.

show ssl-proxy vlan [*vlan-id* | **debug**]

Syntax Description

vlan-id	(Optional) VLAN ID. Displays information for a specific VLAN; valid values are from 1 to 1005.
debug	(Optional) Displays debug information.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all the VLANs configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy vlan
ssl-proxy#
```

Related Commands

show ssl-proxy vlan

snmp-server enable

To configure the SNMP traps and informs, use the **snmp-server enable** command. Use the **no** form of this command to disable SNMP traps and informs.

snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

no snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

Syntax Description

informs	Enables SNMP informs.
traps	Enables SNMP traps.
ipsec	Enables IPSec traps.
isakmp	Enables ISAKMP traps.
snmp	Enables SNMP traps.
ssl-proxy	Enables SNMP SSL proxy notification traps.
cert-expiring	(Optional) Enables SSL proxy certificate-expiring notification traps.
oper-status	(Optional) Enables SSL proxy operation-status notification traps.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to enable SNMP informs:

```
ssl-proxy (config)# snmp-server enable informs
ssl-proxy (config)#
```

This example shows how to enable SSL-proxy traps:

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy
ssl-proxy (config)#
```

This example shows how to enable SSL-proxy notification traps:

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy cert-expiring oper-status
ssl-proxy (config)#
```

ssl-proxy crypto selftest

To initiate a cryptographic self-test, use the **ssl-proxy crypto selftest** command. Use the **no** form of this command to disable the testing.

ssl-proxy crypto selftest [**time-interval** *seconds*]

no ssl-proxy crypto selftest

Syntax Description

time-interval *seconds*	(Optional) Sets the time interval between test cases; valid values are from 1 to 8 seconds.

Defaults

3 seconds

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The **ssl-proxy crypto selftest** command enables a set of crypto algorithm tests to be run on the SSL processor in the background. Random number generation, hashing, encryption and decryption, and MAC generation are tested with a time interval between test cases.

This test is run only for troubleshooting purposes. Running this test will impact run-time performance.

To display the results of the self-test, enter the **show ssl-proxy stats crypto** command.

Examples

This example shows how to start a cryptographic self-test:

```
ssl-proxy (config)# ssl-proxy crypto selftest
ssl-proxy (config)#
```

ssl-proxy mac address

To configure a MAC address, use the **ssl-proxy mac address** command.

ssl-proxy mac address *mac-addr*

Syntax Description

mac-addr	MAC address; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Enter the MAC address in this format: H.H.H.

Examples

This example shows how to configure a MAC address:

```
ssl-proxy (config)# ssl-proxy mac address 00e0.b0ff.f232
ssl-proxy (config)#
```

Related Commands

show ssl-proxy mac address

ssl-proxy natpool

To define a pool of IP addresses, which the Content Switching Module with SSL uses for implementing the client NAT, use the **ssl-proxy natpool** command **.**

ssl-proxy natpool *nat-pool-name start-ip-addr* {**netmask** *netmask*}

Syntax Description

nat-pool-name	NAT pool name.
start-ip-addr	Specifies the first IP address in the pool.
netmask *netmask*	Netmask; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to define a pool of IP addresses:

```
ssl-proxy (config)# ssl-proxy natpool NP2 207.59.10.01 207.59.10.08 netmask 255.0.0.0
ssl-proxy (config)#
```

Related Commands

show ssl-proxy natpool

ssl-proxy pki

To configure and define the PKI implementation on the Content Switching Module with SSL, use the **ssl-proxy pki** command .Use the **no** form of this command to disable the logging and clear the memory .

ssl-proxy pki {{**authenticate** {**timeout** *seconds*}} | {**cache** {{**size** *entries*} | {**timeout** *minutes*}}} | {**certificate** {**check-expiring** {**interval** *hours*}}} | **history**}

no ssl-proxy pki {**authenticate** | **cache** | **certificate** | **history**}

Syntax Description

authenticate	Configures the certificate authentication and authorization.
timeout *seconds*	Specifies the timeout in seconds for each request; valid values are from 1 to 600 seconds.
cache	Configures the peer-certificate cache.
size *entries*	Specifies the maximum number of cache entries; valid values are from 0 to 5000 entries.
timeout *minutes*	Specifies the aging timeout value of entries; valid values are from 1 to 600 minutes.
certificate	Configures the check-expiring interval.
check-expiring interval *hours*	Specifies the check-expiring interval; valid values are from 0 to 720 hours.
history	Key and certificate history.

Defaults

The default settings are as follows:

- **timeout** *seconds*—**180** seconds
- **size** *entries*—**0** entries
- **timeout** *minutes*—**15** minutes
- **interval** *hours*—**0** hours, do not check

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to add the following keywords: • **authenticate** • **cache** • **certificate**
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The**ssl-proxy pki history** command enables logging of certificate history records per-proxy service into memory and generates a syslog message per record. Each record tracks the addition or deletion of a key pair or certificate into the proxy services key and the certificate table.

When the index of the table changes, this command logs the following information:

- Key pair name
- Trustpoint label
- Service name
- Subject name
- Serial number of the certificate

Up to 512 records can be stored in the memory at one time.

Examples

This example shows how to specify the timeout in seconds for each request:

```
ssl-proxy (config)# ssl-proxy pki authenticate timeout 200
ssl-proxy (config)#
```

This example shows how to specify the cache size:

```
ssl-proxy (config)# ssl-proxy pki cache size 50
ssl-proxy (config)#
```

This example shows how to specify the aging timeout value of entries:

```
ssl-proxy (config)# ssl-proxy pki cache timeout 20
ssl-proxy (config)#
```

This example shows how to specify the check-expiring interval:

```
ssl-proxy (config)# ssl-proxy pki certificate check-expiring interval 100
ssl-proxy (config)#
```

This example shows how to enable PKI event-history:

```
ssl-proxy (config)# ssl-proxy pki history
ssl-proxy (config)#
```

Related Commands

show ssl-proxy stats

ssl-proxy policy http-header

To enter the HTTP header insertion configuration submode, use the **ssl-proxy policy http-header** command.

ssl-proxy policy http-header *http-header-policy-name*

Syntax Description

http-header-policy-name	HTTP header policy name.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

In HTTP header insertion configuration submode, you can define the HTTP header insertion content policy that is applied to the payload.

HTTP header insertion allows you to insert additional HTTP headers to indicate to the real server that the connection is actually an SSL connection. These headers allows server applications to collect correct information for each SSL session and/or client.

You can insert these header types:

- Client Certificate—Client certificate header insertion allows the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved. When you specify **client-cert**, the SSL module passes the following headers to the back-end server:
  - Client IP and Port Address—Network address translation (NAT) removes the client IP address and port information. When you specify **client-ip-port**, the SSL module inserts the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port.
  - Custom—When you specify **custom** *custom-string*, the SSL module inserts the user-defined header into the HTTP header.
  - Prefix—When you specify **prefix** *prefix-string*, the SSL module adds the specified prefix into the HTTP header to enable the server to identify that the connections are coming from the SSL module, not from other appliances.
- SSL Session—Session headers, including the session ID, are used to cache client certificates that are based on the session ID. The session headers are also cached on a session basis if the server wants to track connections that are based on a particular cipher suite. When you specify **session**, the SSL module passes information that is specific to an SSL connection to the back-end server as session headers.

Table 3-3 lists the commands available in HTTP header insertion configuration submode.

Table 3-3 HTTP Header Insertion Configuration Submode Command Descriptions

client-cert	Allows the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved.
client-ip-port	Inserts the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port.
custom *custom-string*	Inserts the *custom-string* header into the HTTP header.
prefix	Adds the *prefix-string* to the HTTP header to enable the server to identify the connections that come from the SSL module, not from other appliances.
session	Passes information that is specific to an SSL connection to the back-end server as session headers.

Examples

This example shows how to enter the HTTP header insertion configuration submode:

```
ssl-proxy (config)# ssl-proxy policy http-header test1
ssl-proxy (config-http-header-policy)#
```

This example shows how to allow the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved:

```
ssl-proxy (config-http-header-policy)# client-cert
ssl-proxy (config-http-header-policy)#
```

This example shows how to insert the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port:

```
ssl-proxy (config-http-header-policy)# client-ip-cert
ssl-proxy (config-http-header-policy)#
```

This example shows how to insert the custom-string header into the HTTP header:

```
ssl-proxy (config-http-header-policy)# custom SSL-Frontend:Enable
ssl-proxy (config-http-header-policy)#
```

This example shows how to add the prefix-string into the HTTP header:

```
ssl-proxy (config-http-header-policy)# prefix
ssl-proxy (config-http-header-policy)#
```

This example shows how to pass information that is specific to an SSL connection to the back-end server as session headers:

```
ssl-proxy (config-http-header-policy)# session
ssl-proxy (config-http-header-policy)#
```

Related Commands

show ssl-proxy policy

ssl-proxy policy ssl

To enter the SSL-policy configuration submode, use the **ssl-proxy policy ssl** command. In the SSL-policy configuration submode, you can define the SSL policy for one or more SSL-proxy services .

ssl-proxy policy ssl *ssl-policy-name*

Syntax Description

ssl-policy-name	SSL policy name.

Defaults

The defaults are as follows:

- **cipher** is all.
- **close-protocol** is enabled.
- **session-caching** is enabled.
- **version** is all.
- **session-cache size** *size* is 262143 entries.
- **timeout session** *timeout* is 0 seconds.
- **timeout handshake** *timeout* is 0 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	This command was changed to add the following subcommands: • **session-cache size** *size* • **timeout session** *timeout* [**absolute**]
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Each SSL-policy configuration submode command is entered on its own line.

Table 3-4 lists the commands available in SSL-policy configuration submode.

Table 3-4 SSL-Policy Configuration Submode Command Descriptions

cipher-suite {**RSA_WITH_3DES_EDE_CBC_SHA** | **RSA_WITH_DES_CBC_SHA** | **RSA_WITH_RC4_128_MD5** | **RSA_WITH_RC4_128_SHA** | **all**}	Allows you to configure a list of cipher-suites acceptable to the proxy-server; see the "Usage Guidelines" section for information about the cipher suites.
[**no**] **close-protocol enable**	Allows you to configure the SSL close-protocol behavior. Use the **no** form of this command to disable close protocol.
default {**cipher** | **close-protocol** | **session-cache** | **version**}	Sets a command to its default settings.
exit	Exits from SSL-policy configuration submode.
help	Provides a description of the interactive help system.
[**no**] **session-cache enable**	Allows you to enable the session-caching feature. Use the **no** form of this command to disable session-caching.
session-cache size *size*	Specifies the maximum number of session entries to be allocated for a given service; valid values are from 1 to 262143 entries.
timeout handshake *timeout*	Allows you to configure how long the module keeps the connection in handshake phase; valid values are from 0 to 65535 seconds.
timeout session *timeout* [**absolute**]	Allows you to configure the session timeout. The syntax description is as follows: • *timeout*—Session timeout; valid values are from 0 to 72000 seconds. • **absolute—**(Optional) The session entry is not removed until the configured timeout has completed.
version {**all** | **ssl3** | **tls1**}	Allows you to set the version of SSL to one of the following: • **all**—Both SSL3 and TLS1 versions are used. • **ssl3**—SSL version 3 is used. • **tls1**—TLS version 1 is used.

You can define the SSL policy templates using the **ssl-proxy policy ssl** *ssl-policy-name* command and associate a SSL policy with a particular proxy server using the proxy server configuration CLI. The SSL policy template allows you to define various parameters that are associated with the SSL handshake stack.

When you enable **close-notify**, a close-notify alert message is sent to the client and a close-notify alert message is expected from the client as well. When disabled, the server sends a close-notify alert message to the client; however, the server does not expect or wait for a close-notify message from the client before tearing down the session.

The cipher-suite names follow the same convention as the existing SSL stacks.

The cipher-suites that are acceptable to the proxy-server are as follows:

- RSA_WITH_3DES_EDE_CBC_SHA— RSA with 3des-sha
- RSA_WITH_DES_CBC_SHA—RSA with des-sha
- RSA_WITH_RC4_128_MD5—RSA with rc4-md5

- RSA_WITH_RC4_128_SHA—RSA with rc4-sha
- all—All supported ciphers

If you enter the **timeout session** *timeout* **absolute** command, the session entry is kept in the session cache for the configured timeout before it is cleaned up. If the session cache is full, the timers are active for all the entries, the **absolute** keyword is configured, and all further new sessions are rejected.

If you enter the **timeout session** *timeout* command without the **absolute** keyword, the specified timeout is treated as the maximum timeout and a best-effort is made to keep the session entry in the session cache. If the session cache runs out of session entries, the session entry that is currently being used is removed for incoming new connections.

Examples

This example shows how to enter the SSL-policy configuration submode:

```
ssl-proxy (config)# ssl-proxy policy ssl sslpl1
ssl-proxy (config-ssl-policy)#
```

This example shows how to define the cipher suites that are supported for the SSL-policy:

```
ssl-proxy (config-ssl-policy)# cipher RSA_WITH_3DES_EDE_CBC_SHA
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable the SSL-session closing protocol:

```
ssl-proxy (config-ssl-policy)# close-protocol enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable the SSL-session closing protocol:

```
ssl-proxy (config-ssl-policy)# no close-protocol enable
ssl-proxy (config-ssl-policy)#
```

These examples shows how to set a given command to its default setting:

```
ssl-proxy (config-ssl-policy)# default cipher
ssl-proxy (config-ssl-policy)# default close-protocol
ssl-proxy (config-ssl-policy)# default session-cache
ssl-proxy (config-ssl-policy)# default version
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable session-cache:

```
ssl-proxy (config-ssl-policy)# session-cache enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable session-cache:

```
ssl-proxy (config-ssl-policy)# no session-cache enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to set the maximum number of session entries to be allocated for a given service:

```
ssl-proxy (config-ssl-policy)# session-cache size 22000
ssl-proxy (config-ssl-policy)#
```

This example shows how to configure the session timeout to absolute:

```
ssl-proxy (config-ssl-policy)# timeout session 30000 absolute
ssl-proxy (config-ssl-policy)#
```

These examples show how to enable the support of different SSL versions:

```
ssl-proxy (config-ssl-policy)# version all
ssl-proxy (config-ssl-policy)# version ssl3
ssl-proxy (config-ssl-policy)# version tls1
ssl-proxy (config-ssl-policy)#
```

This example shows how to print out a help page:

```
ssl-proxy (config-ssl-policy)# help
ssl-proxy (config-ssl-policy)#
```

Related Commands

show ssl-proxy stats
show ssl-proxy stats ssl

ssl-proxy policy tcp

To enter the proxy policy TCP configuration submode, use the **ssl-proxy policy tcp** command. In proxy-policy TCP configuration submode, you can define the TCP policy templates.

ssl-proxy policy tcp *tcp-policy-name*

Syntax Description

tcp-policy-name	TCP policy name.

Defaults

The defaults are as follows:

- **timeout inactivity** is 240 seconds.
- **timeout fin-wait** is 600 seconds.
- **buffer-share rx** is 32768 bytes.
- **buffer-share tx** is 32768 bytes.
- **mss** is 1500 bytes.
- **timeout syn** is 75 seconds.
- **timeout reassembly** is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	This command was changed to add the **timeout reassembly** *time* subcommand.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

After you define the TCP policy, you can associate the TCP policy with a proxy server using the proxy-policy TCP configuration submode commands.

Each proxy-policy TCP configuration submode command is entered on its own line.

Table 3-5 lists the commands that are available in proxy-policy TCP configuration submode.

Table 3-5 Proxy-policy TCP Configuration Submode Command Descriptions

default	Sets a command to its default settings.
exit	Exits from proxy-service configuration submode.
[**no**] **timeout fin-wait** *timeout-in-seconds*	Allows you to configure the FIN wait timeout; valid values are from 75 to 600 seconds. Use the **no** form of this command to return to the default setting.
help	Provides a description of the interactive help system.
[**no**] **timeout inactivity** *timeout-in-seconds*	Allows you to configure the inactivity timeout; valid values are from 0 to 960 seconds. This command allows you to set the aging timeout for an idle connection and helps protect the connection resources. Use the **no** form of this command to return to the default setting.
[**no**] **buffer-share rx** *buffer-limit-in-bytes*	Allows you to configure the maximum size of the receive buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting.
[**no**] **buffer-share tx** *buffer-limit-in-bytes*	Allows you to configure the maximum size of the transmit buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting.
[**no**] **mss** *max-segment-size-in-bytes*	Allows you to configure the maximum segment size that the connection identifies in the generated SYN packet; valid values are from 64 to 1460. Use the **no** form of this command to return to the default setting.
[**no**] **timeout syn** *timeout-in-seconds*	Allows you to configure the connection establishment timeout; valid values are from 5 to 75 seconds. Use the **no** form of this command to return to the default setting.
[**no**] **timeout reassembly** *time*	Allows you to configure the amount of time in seconds before the reassembly queue is cleared; valid values are from 0 to 960 seconds (0 = disabled). If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. Use the **no** form of this command to return to the default setting.

Usage Guidelines

TCP commands that you enter on the Content Switching Module with SSL can apply either globally or to a particular proxy server.

You can configure a different maximum segment size for the client side and the server side of the proxy server.

The TCP policy template allows you to define parameters that are associated with the TCP stack.

You can either enter the **no** form of the command or use the **default** keyword to return to the default setting.

Examples

This example shows how to enter the proxy-policy TCP configuration submode:

```
ssl-proxy (config)# ssl-proxy policy tcp tcppl1
ssl-proxy (config-tcp-policy)#
```

These examples show how to set a given command to its default value:

```
ssl-proxy (config-tcp-policy)# default timeout fin-wait
ssl-proxy (config-tcp-policy)# default inactivity-timeout
ssl-proxy (config-tcp-policy)# default buffer-share rx
ssl-proxy (config-tcp-policy)# default buffer-share tx
ssl-proxy (config-tcp-policy)# default mss
ssl-proxy (config-tcp-policy)# default timeout syn
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the FIN-wait timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout fin-wait 200
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the inactivity timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout inactivity 300
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the receive buffer configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share rx 16384
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the transmit buffer configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share tx 13444
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the TCP segment:

```
ssl-proxy (config-tcp-policy)# mss 1460
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the initial connection (SYN)-timeout value:

```
ssl-proxy (config-tcp-policy)# timeout syn 5
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the reassembly-timeout value:

```
ssl-proxy (config-tcp-policy)# timeout reassembly 120
ssl-proxy (config-tcp-policy)#
```

Related Commands

show ssl-proxy policy

ssl-proxy policy url-rewrite

To enter the URL rewrite configuration submode, use the **ssl-proxy policy url-rewrite** command. In URL rewrite configuration submode, you can define the URL-rewrite content policy that is applied to the payload.

ssl-proxy policy url-rewrite *url-rewrite-policy-name*

Syntax Description

url-rewrite-policy-name	URL rewrite policy name.

Defaults

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

URL rewrite allows you to rewrite redirection links only.

A URL rewrite policy consists of up to 32 rewrite rules for each SSL proxy service.

Table 3-6 lists the commands that are available in proxy-policy configuration submode.

Table 3-6 Proxy-policy Configuration Submode Command Descriptions

default	Sets a command to its default settings.
exit	Exits from proxy-policy configuration submode.
help	Provides a description of the interactive help system.
[**no**] **url** *url-string*[**clearport** *port-number* | **sslport** *port-number*]	Allows you to configure the URL string to be rewritten. Use the **no** form of this command to remove the policy.
url-string	Specifies the host portion of the URL link to be rewritten; it can have a maximum of 251 characters. You can use the "*" wildcard only as a prefix or a suffix of a *hostname* in a rewrite rule. For example, you can use the *hostname* in one of the following ways: • www.cisco.com • *.cisco.com • wwwin.cisco.*

Table 3-6 Proxy-policy Configuration Submode Command Descriptions (continued)

clearport *port-number*	(Optional) Specifies the port portion of the URL link that is to be rewritten; valid values are from 1 to 65535.
sslport *port-number*	(Optional) Specifies the *port* portion of the URL link that is to be written; valid values are from 1 to 65535. Enter the **no** form of the command to remove the policy.

Examples

This example shows how to enter the URL rewrite configuration submode for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy#
```

This example shows how to define the URL rewrite policy for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# www.cisco.com clearport 80 sslport 443 redirectonly
ssl-proxy(config-url-rewrite-policy#
```

This example shows how to delete the URL rewrite policy for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# no www.cisco.com clearport 80 sslport 443
redirectonly
ssl-proxy(config-url-rewrite-policy#
```

Related Commands

show ssl-proxy policy

ssl-proxy pool ca

To enter the certificate authority pool configuration submode, use the **ssl-proxy pool ca** command. In the certificate authority pool configuration submode, you can configure a certificate authority pool, which lists the CAs that the module can trust.

ssl-proxy pool *ca-pool-name*

Syntax Description

ca-pool-name	Certificate authority pool name.

Defaults

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

Enter each certificate-authority pool configuration submode command on its own line.

Table 3-7 lists the commands that are available in certificate-authority pool configuration submode.

Table 3-7 Proxy-policy TCP Configuration Submode Command Descriptions

ca	Configures a certificate authority. The available subcommand is as follows: **trustpoint** *ca-trustpoint-name*—Configures a certificate-authority trustpoint. Use the **no** form of this command to return to the default setting.
default	Sets a command to its default settings.
exit	Exits from proxy-service configuration submode.
help	Allows you to configure the connection-establishment timeout; valid values are from 5 to 75 seconds. Use the **no** form of this command to return to the default setting.

Examples

This example shows how to add a certificate-authority trustpoint to a pool:

```
ssl-proxy (config)# ssl-proxy pool test1
ssl-proxy(config-ca-pool)# ca trustpoint test20
ssl-proxy(config-ca-pool)#
```

ssl-proxy service

To enter the proxy-service configuration submode, use the **ssl-proxy-service** command.

ssl-proxy service *ssl-proxy-name* [**client**]

Syntax Description

ssl-proxy-name	SSL proxy name.
client	(Optional) Allows you to configure the SSL-client proxy services. See the **ssl-proxy service client** command.

Defaults

Server NAT is enabled, and client NAT is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the following keywords: • **authenticate**—Configures the certificate verification method. • **client**—Configures the SSL-client proxy services. • **policy urlrewrite—**Applies a URL rewrite policy to a proxy server. • **sslv2**—Enables SSL version 2; see the **server ipaddr** *ip-addr* **protocol** *protocol* **port** *portno* subcommand. • **trusted-ca** *ca-pool-name*—Applies the trusted certificate authority configuration to a proxy server.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

In proxy-service configuration submode, you can configure the virtual IP address and port that is associated with the proxy service and the associated target IP address and port. You can also define TCP and SSL policies for both the client side (beginning with the **virtual** keyword) and the server side of the proxy (beginning with the **server** keyword).

In client proxy-service configuration submode, you specify that the proxy service accept clear-text traffic, encrypt it into SSL traffic, and forward it to the back-end SSL server.

In most cases, all of the SSL-server-proxy configurations that are performed are also valid for the SSL-client-proxy configuration, except for the following:

- You must configure a certificate for the SSL-server-proxy but you do not have to configure a certificate for the SSL-client-proxy. If you configure a certificate for the SSL-client-proxy, that certificate is sent in response to the certificate request message that is sent by the server during the client-authentication phase of the handshake protocol.
- The SSL policy is attached to the virtual subcommand for ssl-server-proxy where as it is attached to server SSL-client-proxy subcommand.

Enter each proxy-service or proxy-client configuration submode command on its own line.

Table 3-8 lists the commands that are available in proxy-service or proxy-client configuration submode.

Table 3-8 Proxy-service Configuration Submode Command Descriptions

Syntax	Description
authenticate verify {**all** | **signature-only**}	Configures the method for certificate verification. You can specify the following: • **all**—Verifies CRLs and signature authority. • **signature-only**—Verifies the signature only.
certificate rsa general-purpose trustpoint *trustpoint-name*	Configures the certificate with RSA general-purpose keys and associates a trustpoint to the certificate.
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	Sets a command to its default settings.
exit	Exits from proxy-service or proxy-client configuration submode.
help	Provides a description of the interactive help system.
inservice	Declares a proxy server or client as administratively up.
nat {**server** | **client** *natpool-name*}	Specifies the usage of either server NAT or client NAT for the server-side connection that is opened by the Content Switching Module with SSL.
policy urlrewrite *policy-name*	Applies a URL rewrite policy to a proxy server.
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword specifies the server that is used for handling SSL version 2 traffic.
server policy tcp *server-side-tcp-policy-name*	Applies a TCP policy to the server side of a proxy server. You can specify the port number and the transport protocol.
trusted-ca *ca-pool-name*	Applies a trusted certificate authenticate configuration to a proxy server.
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} **secondary**	Defines the virtual IP address of the virtual server to which the STE is proxying. You can also specify the port number and the transport protocol. The valid values for *protocol* are **tcp**; valid values for *portno* is from 1 to 65535. The **secondary** keyword (required) prevents the STE from replying to the ARP request coming to the virtual IP address.
virtual {**policy ssl** *ssl-policy-name*}	Applies an SSL policy with the client side of a proxy server.
virtual {**policy tcp** *client-side-tcp-policy-name*}	Applies a TCP policy to the client side of a proxy server.

Both secured and bridge mode between the Content Switching Module (CSM) and the Content Switching Module with SSL is supported.

Use the **secondary** keyword (optional) for bridge-mode topology.

Examples

This example shows how to enter the proxy-service configuration submode:

```
ssl-proxy (config)# ssl-proxy service S6
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the method for certificate verification:

```
ssl-proxy (config-ssl-proxy)# authenticate verify all
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the certificate for the specified SSL-proxy services:

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

This example shows how to apply a trusted-certificate authenticate configuration to a proxy server:

```
ssl-proxy (config-ssl-proxy)# trusted-ca test1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a virtual IP address for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443 secondary
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the SSL policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the TCP policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a clear-text web server for the Content Switching Module with SSL to forward the decrypted traffic:

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a TCP policy for the given clear-text web server:

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a NAT pool for the client address that is used in the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to enable a NAT server address for the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat server
ssl-proxy (config-ssl-proxy)#
```

Related Commands

show ssl-proxy service

ssl-proxy service client

To enter the client proxy-service configuration submode, use the **ssl-proxy service client** command.

ssl-proxy service *ssl-proxy-name* **client**

Syntax Description

ssl-proxy-name	SSL proxy service name.

Defaults

Client NAT is disabled.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

In client proxy-service configuration submode, you specify that the proxy service accept clear-text traffic, encrypt it into SSL traffic, and forward it to the back-end SSL server.

In most cases, all of the SSL-server-proxy configurations that are performed are also valid for the SSL-client-proxy configuration, except for the following:

- You must configure a certificate for the SSL-server-proxy but you do not have to configure a certificate for the SSL-client-proxy. If you configure a certificate for the SSL-client-proxy, that certificate is sent in response to the certificate request message that is sent by the server during the client-authentication phase of handshake protocol.
- The SSL policy is attached to the virtual subcommand for ssl-server-proxy where as it is attached to server SSL-client-proxy subcommand.

Each proxy-service or proxy-client configuration submode command is entered on its own line.

Table 3-9 lists the commands that are available in proxy-client configuration submode.

Table 3-9 Proxy-client Configuration Submode Command Descriptions

Syntax	Description
certificate rsa general-purpose trustpoint *trustpoint-name*	Configures the certificate with RSA general-purpose keys and associates a trustpoint to the certificate.
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	Sets a command to its default settings.
exit	Exits from proxy-client configuration submode.
help	Provides a description of the interactive help system.
inservice	Declares a proxy client as administratively up.

Table 3-9 Proxy-client Configuration Submode Command Descriptions (continued)

Syntax	Description
nat {**server** | **client** *natpool-name*}	Specifies the usage of either server NAT or client NAT for the server side connection that is opened by the Content Switching Module with SSL.
policy urlrewrite *policy-name*	Applies a URL rewrite policy to the proxy server.
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword enables SSL version 2.
server policy tcp *server-side-tcp-policy-name*	Applies a TCP policy to the server side of a proxy server. You can specify the port number and the transport protocol.
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword specifies the server that is used for handling SSL version 2 traffic.
virtual {**policy ssl** *ssl-policy-name*}	Applies an SSL policy with the client side of a proxy server.
virtual {**policy tcp** *client-side-tcp-policy-name*}	Applies a TCP policy to the client side of a proxy server.

Both secured and bridge mode between the Content Switching Module (CSM) and the Content Switching Module with SSL is supported.

Use the **secondary** keyword (optional) for bridge-mode topology.

Examples

This example shows how to enter the client proxy-service configuration submode:

```
ssl-proxy (config)# ssl-proxy service S7 client
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the certificate for the specified SSL-proxy services:

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a virtual IP address for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the SSL policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the TCP policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a clear-text web server for the Content Switching Module with SSL to forward the decrypted traffic:

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a TCP policy for the given clear-text web server:

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a NAT pool for the client address that is used in the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to enable a NAT server address for the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat server
ssl-proxy (config-ssl-proxy)#
```

Related Commands

show ssl-proxy service

ssl-proxy ssl ratelimit

To prohibit new connections during overload conditions, use the **ssl-proxyy ssl ratelimit** command. Use the **no** form of this command to allow new connections if memory is available.

ssl-proxyy ssl ratelimit

no ssl-proxyy ssl ratelimit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Examples

This example shows how to prohibit new connections during overload conditions:

```
ssl-proxy (config)# ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

This example shows how to allow new connections during overload conditions if memory is available:

```
ssl-proxy (config)# no ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

ssl-proxy vlan

To enter the proxy-VLAN configuration submode, use the **ssl-proxy vlan** command. In proxy-VLAN configuration submode, you can configure a VLAN for the Content Switching Module with SSL.

ssl-proxy vlan *vlan*

Syntax Description

vlan	VLAN ID; valid values are from 1 to 1005.

Defaults

The defaults are as follows:

- *hellotime* is 3 seconds.
- *holdtime* is 10 seconds.
- *priority* is 100.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the **standby** keyword and arguments to configure HSRP.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

VLAN 1 is not supported by the CSM.

Extended-range VLANs are not supported by the Content Switching Module with SSL.

Enter each proxy-VLAN configuration submode command on its own line.

Table 3-10 lists the commands that are available in proxy-VLAN configuration submode.

Table 3-10 Proxy-VLAN Configuration Submode Command Descriptions

Syntax	Description
admin	Configures the VLAN as an administration VLAN.
exit	Exits from the proxy-VLAN configuration submode.
gateway *prefix* [**drop** | **forward**[1]]	Configures the VLAN with a gateway to the Internet.
help	Provides a description of the interactive help system.
ipaddr *prefix mask*	Configures the VLAN with an IP address and a subnet mask.
no	Negates a command or sets its defaults.

Table 3-10 Proxy-VLAN Configuration Submode Command Descriptions (continued)

Syntax	Description
route {*prefix mask*} {**gateway** *prefix*}	Configures a gateway so that the Content Switching Module with SSL can reach a nondirect connected subnetwork.
standby [*group-number*] {**authentication text** *string*} | {**delay minimum** [*min-delay*] **reload** [*reload-delay*]} | {**ip** [*ip-address* [**secondary**]]} | {**mac-address** *mac-address*} | {**mac-refresh** *seconds*} | {**name** *group-name*} | {**preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]} | {**priority** *priority*} | {**redirects** [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]} | {**timers** [**msec**] *hellotime* [**msec**] *holdtime*} | {**track** *object-number* [**decrement** *priority*]}	Configures redundancy on the VLAN. See the following commands for valid values: • **standby authentication** • **standby delay minimum reload** • **standby ip** • **standby mac-address** • **standby mac-refresh** • **standby name** • **standby preempt** • **standby priority** • **standby redirects** • **standby timers** • **standby track** • **standby use-bia**

[1] The gateway forward feature from the SSL Services Module does not work with CSM-S because the SSL daughter card only gets packets for connections that are being serviced by a VIP on the CSM.

You must remove the administration VLAN status of the current administration VLAN before you can configure a different administration VLAN.

An administration VLAN is used for communication with the certificate agent (PKI) and the management station (SNMP).

When configuring the gateway, the **drop** keyword allows the Content Switching Module with SSL to drop a packet if a virtual service cannot be found relating to the packet.

When configuring the gateway, the **forward** keyword allows the Content Switching Module with SSL to forward a packet to the gateway of the specified VLAN if a virtual service cannot be found relating to the packet.

The valid values for configuring HSRP are as follows:

- *group-number*—(Optional) Group number on the interface for which HSRP is being activated; valid values are from 0 to 255. If you do not specify a *group-number*, group **0** is used.
- **ip** *ip-addr*—Specifies the IP address of the HSRP interface.
- **priority** *priority*— Specifies the priority for the HSRP interface. Increase the priority of at least one interface in the HSRP group. The interface with the highest priority becomes active for that HSRP group.
- **prempt** —Enables preemption. When you enable preemption, if the local router has a hot standby priority that is higher than the current active router, the local router attempts to assume control as the active router. If you do not configure preemption, the local router assumes control as the active router only if it receives information indicating that no router is in the active state (acting as the designated router).

- **delay**—(Optional) Specifies the preemption delay. When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it becomes the active router but cannot provide adequate routing services. You can configure a delay before the preempting router actually preempts the currently active router.
- *type time*—Specifies the preemption type and delay; valid values are as follows:
  - **minimum** *time*—Specifies the minimum delay period in delay seconds; valid values are from 0 to 3600 seconds (1 hour).
  - **reload** *time*—Specifies the preemption delay after a reload only.
  - **sync** *time*—Specifies the maximum synchronization period in delay seconds.
- **timers** [**msec**] *hellotime holdtime*—Configures the time between hello packets and the time before other routers declare the active hot standby or standby router to be down; valid values are as follows:
  - **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
  - *hellotime*—Hello interval (in seconds); valid values are from 1 to 254 seconds. If you specify the **msec** keyword, the hello interval is in milliseconds; valid values are from 15 to 999 milliseconds. The default is 3 seconds.
  - *holdtime*—Time (in seconds) before the active or standby router is declared to be down; valid values are from x to 255. If you specify the **msec** keyword, the holdtime is in milliseconds; valid values are from y to 3000 milliseconds. The default is 10 seconds.

    Where:

    x is the *hellotime* plus 50 milliseconds and is rounded up to the nearest 1 second.

    y is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

Examples

This example shows how to enter the proxy-VLAN configuration submode:

```
ssl-proxy (config)# ssl-proxy vlan 6
ssl-proxy (config-vlan)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-vlan)# default admin
ssl-proxy (config-vlan)# default gateway
ssl-proxy (config-vlan)# default ipaddr
ssl-proxy (config-vlan)# default route
```

This example shows how to configure the specified VLAN with a gateway:

```
ssl-proxy (config-vlan)# gateway 209.0.207.5
ssl-proxy (config-vlan)#
```

This example shows how to configure the specified VLAN with an IP address and subnet mask:

```
ssl-proxy (config-vlan)# ipaddr 208.59.100.18 255.0.0.0
ssl-proxy (config-vlan)#
```

This example shows how to configure a gateway for the Content Switching Module with SSL to reach a nondirect subnetwork:

```
ssl-proxy (config-vlan)# route 210.0.207.0 255.0.0.0 gateway 209.0.207.6
ssl-proxy (config-vlan)#
```

This example shows how to configure the HSRP on the SSL module:

```
ssl-proxy(config)# ssl-proxy vlan 100
ssl-proxy(config-vlan)# ipaddr 10.1.0.20 255.255.255.0
```

```
ssl-proxy(config-vlan)# gateway 10.1.0.1
ssl-proxy(config-vlan)# admin
ssl-proxy(config-vlan)# standby 1 ip 10.1.0.21
ssl-proxy(config-vlan)# standby 1 priority 110
ssl-proxy(config-vlan)# standby 1 preempt
ssl-proxy(config-vlan)# standby 2 ip 10.1.0.22
ssl-proxy(config-vlan)# standby 2 priority 100
ssl-proxy(config-vlan)# standby 2 preempt
ssl-proxy(config-vlan)# end
ssl-proxy#
```

Related Commands

show ssl-proxy vlan

standby authentication

To configure an authentication string for HSRP, use the **standby authentication** command. Use the **no** form of this command to delete an authentication string.

standby [*group-number*] **authentication text** *string*

no standby [*group-number*] **authentication text** *string*

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies.
text *string*	Authentication string, which can be up to eight characters.

Defaults

The defaults are as follows:

- *group-number* is **0**.
- *string* is **cisco**.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

HSRP ignores unauthenticated HSRP messages.

The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated hot standby IP address and the hot standby timer values from the other routers that are configured with HSRP.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

Examples

This example shows how to configure “word” as the authentication string to allow hot standby routers in group 1 to interoperate:

```
ssl-proxy (config-vlan)# standby 1 authentication text word
ssl-proxy (config-vlan)#
```

standby delay minimum reload

To configure a delay before the HSRP groups are initialized, use the **standby delay minimum reload** command. Use the **no** form of this command to disable the delay.

standby delay minimum [*min-delay*] **reload** [*reload-delay*]

no standby delay minimum [*min-delay*] **reload** [*reload-delay*]

Syntax Description

min-delay	(Optional) Minimum time (in seconds) to delay HSRP group initialization after an interface comes up.
reload-delay	(Optional) Time (in seconds) to delay after the router has reloaded.

Defaults

The defaults are as follows:

- *min-delay* is **1** second.
- *reload-delay* is **5** seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *min-delay* applies to all subsequent interface events.

The *reload-delay* applies only to the first interface-up event after the router has reloaded.

If the active router fails or you remove it from the network, the standby router automatically becomes the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, in some cases, even if you do not use the **standby preempt** command, the former active router resumes the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay for HSRP group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through and configuring longer delay values is not necessary.

The delay is canceled if an HSRP packet is received on an interface.

Examples

This example shows how to set the minimum delay to 30 seconds and the delay after the first reload to 120 seconds:

```
ssl-proxy (config-vlan)# standby delay minimum 30 reload 120
ssl-proxy (config-vlan)#
```

Related Commands

show standby delay
standby preempt
standby timers

standby ip

To activate HSRP, use the **standby ip** command. Use the **no** form of this command to disable HSRP.

standby [*group-number*] **ip** [*ip-address* [**secondary**]]

no standby [*group-number*] **ip** [*ip-address*]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated.
ip-address	(Optional) IP address of the hot standby router interface.
secondary	(Optional) Indicates the IP address is a secondary hot standby router interface.

Defaults

The defaults are as follows:

- *group-number* is 0.
- HSRP is disabled by default.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The **standby ip** command allows you to configure primary and secondary HSRP addresses.

The **standby ip** command activates HSRP on the configured interface. If you specify an IP address, that address is used as the designated address for the hot standby group. If you do not specifiy an IP address, the designated address is learned through the standby function. So that HSRP can elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When you enable the **standby ip** command on an interface, the handling of proxy ARP requests is changed (unless proxy ARP was disabled). If the hot standby state of the interface is active, proxy ARP requests are answered using the MAC address of the hot standby group. If the interface is in a different state, proxy ARP responses are suppressed.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

Examples

This example shows how to activate HSRP for group 1 on Ethernet interface 0. The IP address that is used by the hot standby group is learned using HSRP.

```
ssl-proxy (config-vlan)# standby 1 ip
ssl-proxy (config-vlan)#
```

This example shows how to indicate that the IP address is a secondary hot standby router interface:

```
ssl-proxy (config-vlan)# standby ip 1.1.1.254
ssl-proxy (config-vlan)# standby ip 1.2.2.254 secondary
ssl-proxy (config-vlan)# standby ip 1.3.3.254 secondary
```

standby mac-address

To specify a virtual MAC address for HSRP, use the **standby mac-address** command. Use the **no** form of this command to revert to the standard virtual MAC address (0000.0C07.AC*xy)*.

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
mac-address	MAC address.

Defaults

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command cannot be used on a Token Ring interface.

You can use HSRP to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, it is often necessary to be able to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **standby mac-address** command to specify the virtual MAC address.

The specified MAC address is used as the virtual MAC address when the router is active.

This command is intended for certain APPN configurations. The parallel terms are shown in Table 3-11.

Table 3-11 Parallel Terms Between APPN and IP

APPN	IP
End node	Host
Network node	Router or gateway

In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **standby mac-address** command in the routers to set the virtual MAC address to the value that is used in the end nodes.

Examples

This example shows how to configure HSRP group 1 with the virtual MAC address:

```
ssl-proxy (config-vlan)# standby 1 mac-address 4000.1000.1060
ssl-proxy (config-vlan)#
```

Related Commands

show standby
standby use-bia

standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI, use the **standby mac-refresh** command. Use the **no** form of this command to restore the default value.

standby mac-refresh *seconds*

no standby mac-refresh

Syntax Description

seconds	Number of seconds in the interval at which a packet is sent to refresh the MAC cache; valid values are from 1 to 255 seconds.

Defaults

seconds is **10** seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command applies to HSRP running over FDDI only. Packets are sent every 10 seconds to refresh the MAC cache on learning bridges or switches. By default, the MAC cache entries age out in 300 seconds (5 minutes).

All other routers participating in HSRP on the FDDI ring receive the refresh packets, although the packets are intended only for the learning bridge or switch. Use this command to change the interval. Set the interval to 0 if you want to prevent refresh packets (if you have FDDI but do not have a learning bridge or switch).

Examples

This example shows how to change the MAC-refresh interval to 100 seconds. In this example, a learning bridge needs to miss three packets before the entry ages out.

```
ssl-proxy (config-vlan)# standby mac-refresh 100
ssl-proxy (config-vlan)#
```

standby name

To configure the name of the standby group, use the **standby name** command. Use the **no** form of this command to disable the name.

standby name *group-name*

no standby name *group-name*

Syntax Description

group-name	Specifies the name of the standby group.

Defaults

HSRP is disabled.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *group-name* argument specifies the HSRP group.

Examples

This example shows how to specifiy the standby name as SanJoseHA:

```
ssl-proxy (config-vlan)# standby name SanJoseHA
ssl-proxy (config-vlan)#
```

Related Commands

ip mobile home-agent redundancy (refer to the *Cisco IOS Release 12.2 Command Reference)*

standby preempt

To configure HSRP preemption and preemption delay, use the **standby preempt** command. Use the **no** form of this command to restore the default values.

standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

no standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *delay*	(Optional) Specifies the minimum delay in *delay* seconds; valid values are from 0 to 3600 seconds (1 hour).
reload *delay*	(Optional) Specifies the preemption delay after a reload only.
sync *delay*	(Optional) Specifies the maximum synchronization period in *delay* seconds.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *delay* is 0 seconds; the router preempts immediately. By default, the router that comes up later becomes the standby router.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The *delay* argument causes the local router to postpone taking over the active role for *delay* (minimum) seconds since that router was last restarted.

When you use this command, the router is configured to preempt, which means that when the local router has a hot standby priority that is higher than the current active router, the local router should attempt to assume control as the active router. If you do not configure preemption, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If you configure the router to preempt, it becomes the active router, but it cannot provide adequate routing services. You can configure a delay before the preempting router actually preempts the currently active router.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

IP-redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *delay* command specifies a maximum number of seconds to allow IP-redundancy clients to prevent preemption. When this expires, preemption takes place regardless of the state of the IP-redundancy clients.

The **standby preempt delay reload** *delay* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command disables the preemption delay but preemption remains enabled. The **no standby preempt delay minimum** *delay* command disables the minimum delay but leaves any synchronization delay if it was configured.

Examples

This example shows how to configure the router to wait for 300 seconds (5 minutes) before attempting to become the active router:

```
ssl-proxy (config-vlan)# standby preempt delay minimum 300
ssl-proxy (config-vlan)#
```

standby priority

To configure the priority for HSRP, use the **standby priority** command. Use the **no** form of this command to restore the default values.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
priority	Priority value that prioritizes a potential hot standby router; valid values are from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *priority* is 100.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The router in the HSRP group with the highest priority value becomes the active router.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.

Examples

This example shows how to change the router priority:

```
ssl-proxy (config-vlan)# standby priority 120
ssl-proxy (config-vlan)#
```

Examples

standby track

standby redirects

To enable HSRP filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirects** command. Use the **no** form of this command to disable the HSRP filtering of ICMP redirect messages.

standby redirects [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

no standby redirects [**unknown**]

Syntax Description

enable	(Optional) Allows the filtering of ICMP redirect messages on interfaces that are configured with HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.
disable	(Optional) Disables the filtering of ICMP redirect messages on interfaces that are configured with HSRP.
timers	(Optional) Adjusts HSRP-router advertisement timers.
advertisement	(Optional) HSRP-router advertisement interval in seconds; valid values are from 10 to 180 seconds.
holddown	(Optional) HSRP-router holddown interval in seconds; valid values are from 61 to 3600.
unknown	(Optional) Allows sending of ICMP packets to be sent when the next-hop IP address that is contained in the packet is unknown in the HSRP table of real IP addresses and active virtual IP addresses.

Defaults

The defaults are as follows:

- HSRP filtering of ICMP redirect messages is enabled if you configure HSRP on an interface.
- *advertisement* is 60 seconds.
- *holddown* is 180 seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can configure the **standby redirects** command globally or on a per-interface basis. When you first configure HSRP on an interface, the setting for that interface inherits the global value. If you explicitly disable the filtering of ICMP redirects on an interface, then the global command cannot reenable this functionality.

The **no standby redirects** command is the same as the **standby redirects disable** command. We do not recommend that you save the **no** form of this command to NVRAM. Because the command is enabled by default, we recommend that you use the **standby redirects disable** command to disable the functionality.

With the **standby redirects** command enabled, the real IP address of a router can be replaced with a virtual IP address in the next-hop address or gateway field of the redirect packet. HSRP looks up the next-hop IP address in its table of real IP addresses versus virtual IP addresses. If HSRP does not find a match, the HSRP router allows the redirect packet to go out unchanged. The host HSRP router is redirected to a router that is unknown, that is, a router with no active HSRP groups. You can specify the **no standby redirects unknown** command to stop these redirects from being sent.

Examples

This example shows how to allow HSRP to filter ICMP redirect messages:

```
ssl-proxy (config-vlan)# standby redirects
ssl-proxy (config-vlan)#
```

This example shows how to change the HSRP router advertisement interval to 90 seconds and the holddown timer to 270 seconds on interface Ethernet 0:

```
ssl-proxy (config-vlan)# standby redirects timers 90 270
ssl-proxy (config-vlan)#
```

Related Commands

show standby
show standby redirect

standby timers

To configure the time between hello packets and the time before other routers declare the active hot standby or standby router to be down, use the **standby timers** command. Use the **no** form of this command to return to the default settings.

standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply.
msec	(Optional) Interval in milliseconds.
hellotime	Hello interval (in seconds); see the "Usage Guidelines" section for valid values.
holdtime	Time (in seconds) before the active or standby router is declared to be down; see the "Usage Guidelines" section for valid values.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *hellotime* is 3 seconds.
- *holdtime* is 10 seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

The valid values for *hellotime* are as follows:

- If you did not enter the **msec** keyword, valid values are from 1 to 254 seconds.
- If you enter the **msec** keyword, valid values are from 15 to 999 milliseconds.

The valid values for *holdtime* are as follows:

- If you did not enter the **msec** keyword, valid values are from *x* to 255 seconds, where *x* is the *hellotime* and 50 milliseconds and is rounded up to the nearest 1 second.
- If you enter the **msec** keyword, valid values are from *y* to 3000 milliseconds, where *y* is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

If you specify the **msec** keyword, the hello interval is in milliseconds. Millisecond timers allow for faster failover.

The **standby timers** command configures the time between standby hello packets and the time before other routers declare the active or standby router to be down. Routers or access servers on which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, holdtime is greater than or equal to 3 times the value of hellotime. The range of values for holdtime force the holdtime to be greater than the hellotime. If the timer values are specified in milliseconds, the holdtime is required to be at least three times the hellotime value and not less than 50 milliseconds.

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used on Cisco 7200 platforms or better, and on Fast-Ethernet or FDDI interfaces or better. Setting the **process-max-time** command to a suitable value may also help with flapping.

The value of the standby timer will not be learned through HSRP hellos if it is less than 1 second.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

This example sets, for group number 1 on Ethernet interface 0, the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds:

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

This example sets, for the hot router interface that is located at 172.19.10.1 on Ethernet interface 0, the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds:

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

This example sets, for the hot router interface that is located at 172.18.10.1 on Ethernet interface 0, the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds. Note that the holdtime is three times larger than the hellotime because the minimum holdtime value in milliseconds is 50.

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

standby track

To configure HSRP to track an object and change the hot standby priority based on the state of the object, use the **standby track** command. Use the **no** form of this command to remove the tracking.

standby [*group-number*] **track** *object-number* [**decrement** *priority*]

no standby [*group-number*] **track** *object-number* [**decrement** *priority*]

Syntax Description

group-number	(Optional) Group number to which the tracking applies.
object-number	Object number in the range from 1 to 500 representing the object to be tracked.
decrement *priority*	(Optional) Amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up).

Defaults

The defaults are as follows:

- *group-number* is **0**.
- *priority* is **10**.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

This command ties the hot standby priority of the router to the availability of its tracked objects. Use the **track interface** or **track ip route** global configuration command to track an interface object or an IP route object. The HSRP client can register its interest in the tracking process by using the **standby track** command commands and take action when the object changes.

When a tracked object goes down, the priority decreases by 10. If an object is not tracked, its state changes do not affect the priority. For each object configured for hot standby, you can configure a separate list of objects to be tracked.

The optional *priority* argument specifies how much to decrement the hot standby priority when a tracked object goes down. When the tracked object comes back up, the priority is incremented by the same amount.

When multiple tracked objects are down, the decrements are cumulative, whether configured with *priority* values or not.

Use the **no standby** *group-number* **track** command to delete all tracking configuration for a group.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

The **standby track** command syntax prior to Release 12.2(15)T is still supported. Using the older form will cause a tracked object to be created in the new tracking process. This tracking information can be displayed using the **show track** command.

Examples

This example shows how to track the IP routing capability of serial interface 1/0. HSRP on Ethernet interface 0/0 registers with the tracking process to be informed of any changes to the IP routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Router A becomes the HSRP active router because it has the higher priority.

However, if IP routing on serial interface 1/0 in Router A fails, the HSRP group priority is reduced and Router B takes over as the active router, which maintains a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Router A Configuration

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.21 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 105
  standby 1 track 100 decrement 10
```

Router B Configuration

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.22 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 100
  standby 1 track 100 decrement 10
```

Related Commands

standby preempt
standby priority

standby use-bia

To configure HSRP to use the burned-in address of the interface as its virtual MAC address instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** command. Use the **no** form of this command to restore the default virtual MAC address.

standby use-bia [**scope interface**]

no standby use-bia

Syntax Description

scope interface	(Optional) Specifies that this command is configured only for the subinterface on which it was entered, instead of the major interface.

Defaults

HSRP uses the preassigned MAC address on Ethernet and FDDI or the functional address on Token Ring.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
CSM-S release 1.1(1)	This command was introduced.

Usage Guidelines

You can configure multiple standby groups on an interface when you enter the **standby use-bia** command. Hosts on the interface must have a default gateway configured. We recommend that you set the **no ip proxy-arp** command on the interface. We also recommend that you configure the **standby use-bia** command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses that are set to a functional address.

When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

Without the **scope interface** keywords, the **standby use-bia** command applies to all subinterfaces on the major interface. You cannot enter the **standby use-bia** command both with and without the **scope interface** keywords at the same time.

Examples

This example shows how to map the virtual MAC address to the virtual IP address:

```
ssl-proxy (config-vlan)# standby use-bia
ssl-proxy (config-vlan)#
```

Acronyms

Table A-1 defines the acronyms that are used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
ACNS	Application and Content Networking System
AFI	authority and format identifier
Agport	aggregation port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode
AV	attribute value
BDD	binary decision diagrams
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
Bidir	bidirectional PIM
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface
CAM	content-addressable memory
CAR	committed access rate

Table A-1 List of Acronyms (continued)

Acronym	Expansion
CBAC	context based access control
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CIST	Common and Internal Spanning Tree
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
CNS	Cisco Networking Services
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CSM	Content Switching Module
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility
DEC	Digital Equipment Corporation
DF	designated forwarder
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DoS	denial of service

Table A-1 List of Acronyms (continued)

Acronym	Expansion
dot1q	802.1Q
dot1x	802.1x
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DXI	data exchange interface
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EHSA	enhanced high system availability
EIA	Electronic Industries Association
ELAN	Emulated Local Area Network
EOBC	Ethernet out-of-band channel
EOF	end of file
EoMPLS	Ethernet over Multiprotocol Label Switching
ESI	end-system identifier
FAT	File Allocation Table
FIB	Forwarding Information Base
FIE	Feature Interaction Engine
FECN	forward explicit congestion notification
FM	feature manager
FRU	field replaceable unit
fsck	file system consistency check
FSM	feasible successor metrics
FSU	fast software upgrade
FWSM	Firewall Services Module
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-card Communication or interface controller card

Table A-1 List of Acronyms (continued)

Acronym	Expansion
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDSM	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGMPv2	IGMP version 2
IGMPv3	IGMP version 3
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISL VLANs	Inter-Switch Link VLANs
ISO	International Organization of Standardization
ISR	Integrated SONET router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol data unit
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server
LLC	Logical Link Control
LOU	logical operation units
LTL	Local Target Logic
MAC	Media Access Control

Table A-1 List of Acronyms (continued)

Acronym	Expansion
MD5	message digest 5
MDIX	media-dependent interface crossover
MDSS	Multicast Distributed Shortcut Switching
MFD	multicast fast drop
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MLSM	multilayer switching for multicast
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MPLS	Multiprotocol Label Switching
MRM	multicast routing monitor
MSDP	Multicast Source Discovery Protocol
MSFC	Multilayer Switching Feature Card
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree (802.1s)
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NDR	no drop rate
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVGEN	nonvolatile generation
NVRAM	nonvolatile RAM
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OIF	Outgoing interface of a multicast {*,G} or {source, group} flow

Table A-1 List of Acronyms (continued)

Acronym	Expansion
OSI	Open System Interconnection
OSM	Optical Services Module
OSPF	open shortest path first
PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PBR	policy-based routing
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point
PFC	Policy Feature Card
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	protocol independent multicast
PPP	Point-to-Point Protocol
ppsec	packets per second
PRID	Policy Rule Identifiers
PVLANs	private VLANs
PVST+	Per-VLAN Spanning Tree+
QDM	QoS device manager
QM	QoS manager
QM-SP	SP QoS manager
QoS	quality of service
Q-in-Q	802.1Q in 802.1Q
RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol
RIB	routing information base
RIF	Routing Information Field

Table A-1 List of Acronyms (continued)

Acronym	Expansion
RMON	remote network monitor
ROM	read-only memory
ROMMON	ROM monitor
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy+
RSPAN	remote SPAN
RST	reset
RSTP	Rapid Spanning Tree Protocol
RSTP+	Rapid Spanning Tree Protocol plus
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SFP	small form factor pluggable
SGBP	Stack Group Bidding Protocol
SIMM	single in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SREC	S-Record format, Motorola defined format for ROM contents
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
SSTP	Cisco Shared Spanning Tree

Table A-1 List of Acronyms (continued)

Acronym	Expansion
STP	Spanning Tree Protocol
SVC	switched virtual circuit
SVI	switched virtual interface
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	table contention level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TopN	Utility that allows the user to analyze port traffic by reports
ToS	type of service
TLV	type-length-value
TTL	Time To Live
TVX	valid transmission
UDLD	UniDirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel circuit
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VMR	value mask result
VPN	virtual private network
VRF	VPN routing and forwarding
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID
WAN	wide area network
WCCP	Web Cache Coprocessor Protocol
WFQ	weighted fair queueing
WRED	weighted random early detection

Table A-1 List of Acronyms (continued)

Acronym	Expansion
WRR	weighted round-robin
XNS	Xerox Network System

INDEX