Catalyst 6500 Series Switch Content Switching Module Command Reference

Software Release 4.2(x)
December, 2006

WS-X6066-SLB-APC

Americas 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: 408 527-0883

Text Part Number: OL-6897-01

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Catalyst 6500 Series Content Switching Module Command Reference
Copyright ©2005-2006, Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Audience ix

Organization ix

Conventions x

Related Documentation xi

Obtaining Documentation xi

Cisco.com xi

Product Documentation DVD xi

Ordering Documentation xi

Documentation Feedback xii

Cisco Product Security Overview xii

Reporting Security Problems in Cisco Products xii

Product Alerts and Field Notices xiii

Obtaining Technical Assistance xiii

Cisco Support Website xiii

Submitting a Service Request xiv

Definitions of Service Request Severity xiv

Obtaining Additional Publications and Information xv

CHAPTER 1 **Using Content Switching Module Commands** 1-1

Using the CSM Commands 1-1

Command Modes 1-2

Regular Expressions 1-3

CHAPTER 2 **Content Switching Module Commands** 2-1

arp 2-2

capp udp 2-3

options (CAPP UDP submode) 2-5

port (CAPP UDP submode) 2-6

secure (CAPP UDP submode) 2-7

clear module csm 2-8

dfp 2-9

agent (DFP submode) **2-10**
manager (DFP submode) **2-11**
exit **2-12**
ft group **2-13**
failover (fault tolerant submode) **2-15**
heartbeat-time (fault tolerant submode) **2-16**
preempt (fault tolerant submode) **2-17**
track (fault tolerant submode) **2-18**
priority (fault tolerant submode) **2-19**
hw-module csm standby config-sync **2-20**
ip slb mode **2-21**
map cookie **2-23**
match protocol http cookie (cookie map submode) **2-24**
map dns **2-25**
match protocol dns domain (DNS map submode) **2-26**
map header **2-27**
insert protocol http header (header map submode) **2-28**
match protocol http header (header map submode) **2-29**
map retcode **2-30**
match protocol http retcode (return code map submode) **2-31**
map url **2-32**
match protocol http url (URL map submode) **2-33**
module csm **2-34**
natpool (module CSM submode) **2-35**
variable (module CSM submode) **2-36**
owner **2-41**
billing-info (owner submode) **2-42**
contact-info (owner submode) **2-43**
maxconns (owner submode) **2-44**
policy **2-45**
client-group (policy submode) **2-46**
cookie-map (policy submode) **2-47**
header-map (policy submode) **2-48**
nat client (policy submode) **2-49**
serverfarm (policy submode) **2-50**

set ip dscp (policy submode) **2-52**
sticky-group (policy submode) **2-53**
url-map (policy submode) **2-54**
probe **2-55**
address (probe submode) **2-57**
credentials (probe submode) **2-58**
description (serverfarm submode) **2-59**
expect status (probe submode) **2-60**
failed (probe submode) **2-62**
header (probe submode) **2-63**
interval (probe submode) **2-64**
name (probe submode) **2-65**
open (probe submode) **2-66**
port (probe submode) **2-67**
receive (probe submode) **2-68**
recover (probe submode) **2-69**
request (probe submode) **2-70**
retries (probe submode) **2-71**
script (probe submode) **2-72**
real **2-73**
address (real server submode) **2-76**
backup real (real server submode) **2-77**
health probe (real server submode) **2-78**
inservice (real server submode) **2-79**
location (real server submode) **2-81**
maxconns (real server submode) **2-82**
minconns (real server submode) **2-83**
redirect-vserver (real server submode) **2-84**
weight (real server submode) **2-85**
redirect-vserver **2-86**
advertise (redirect virtual server submode) **2-87**
client (redirect virtual server submode) **2-88**
idle (redirect virtual server submode) **2-89**
inservice (redirect virtual server submode) **2-90**
replicate csrp (redirect virtual server submode) **2-91**

ssl (redirect virtual server submode) **2-92**
virtual (redirect virtual server submode) **2-93**
vlan (redirect virtual server submode) **2-94**
webhost backup (redirect virtual server submode) **2-95**
webhost relocation (redirect virtual server submode) **2-96**
reverse-sticky **2-97**
script file **2-98**
script task **2-100**
serverfarm **2-101**
bindid (serverfarm submode) **2-102**
description (serverfarm submode) **2-103**
failaction (serverfarm submode) **2-104**
health (serverfarm submode) **2-105**
nat client (serverfarm submode) **2-106**
nat server (serverfarm submode) **2-107**
predictor (serverfarm submode) **2-108**
probe (serverfarm submode) **2-111**
real (serverfarm submode) **2-112**
real name (serverfarm submode) **2-114**
retcode-map (serverfarm submode) **2-116**
show module csm **2-117**
show module csm arp **2-118**
show module csm capp **2-119**
show module csm conns **2-121**
show module csm dfp **2-123**
show module csm ft **2-125**
show module csm map **2-126**
show module csm memory **2-128**
show module csm natpool **2-129**
show module csm owner **2-130**
show module csm policy **2-131**
show module csm probe **2-132**
show module csm probe script **2-133**
show module csm pvlan **2-134**
show module csm real **2-135**

show module csm real retcode **2-138**
show module csm script **2-139**
show module csm script task **2-140**
show module csm serverfarm **2-141**
show module csm static **2-143**
show module csm static server **2-144**
show module csm stats **2-145**
show module csm status **2-148**
show module csm sticky **2-149**
show module csm tech-script **2-151**
show module csm tech-support **2-152**
show module csm variable **2-155**
show module csm vlan **2-157**
show module csm vserver redirect **2-158**
show module csm xml stats **2-159**
snmp enable traps slb ft **2-160**
static **2-161**
real (static NAT submode) **2-162**
sticky **2-163**
cookie offset (sticky submode) **2-165**
cookie secondary (sticky submode) **2-166**
header (sticky submode) **2-167**
static (sticky submode) **2-168**
vserver **2-169**
advertise (virtual server submode) **2-170**
client (virtual server submode) **2-171**
description (virtual server submode) **2-172**
domain (virtual server submode) **2-173**
idle (virtual server submode) **2-174**
inservice (virtual server submode) **2-175**
owner (virtual server submode) **2-176**
parse-length (virtual server submode) **2-177**
pending (virtual server submode) **2-178**
persistent rebalance (virtual server submode) **2-179**
replicate csrp (virtual server submode) **2-180**

reverse-sticky (virtual server submode) **2-181**
serverfarm (virtual server submode) **2-182**
slb-policy (virtual server submode) **2-184**
ssl-sticky (virtual server submode) **2-185**
status-tracking (virtual server submode) **2-186**
sticky (virtual server submode) **2-187**
url-hash (virtual server submode) **2-189**
virtual (virtual server submode) **2-190**
unidirectional (virtual server submode) **2-192**
vlan (virtual server submode) **2-193**
vlan **2-194**
alias (VLAN submode) **2-195**
description (VLAN submode) **2-197**
gateway (VLAN submode) **2-198**
ip address (VLAN submode) **2-199**
route (VLAN submode) **2-200**
xml-config **2-201**
client-group (XML submode) **2-202**
credentials (XML submode) **2-203**
inservice (XML submode) **2-204**
port (XML submode) **2-205**
vlan (XML submode) **2-206**

INDEX

Preface

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

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

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

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 Commands	Provides detailed descriptions of all commands in alphabetical listing.

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 arguments; 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

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/mod_icn/csm/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. This section explains the product documentation resources that Cisco offers.

Cisco.com

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

http://www.cisco.com/techsupport

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

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco 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 at this URL:

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

Access to all tools on the Cisco 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 Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 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 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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

- *Internet Protocol Journal* is a quarterly journal published by Cisco 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

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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 commands and contains the following sections:

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

Using the CSM Commands

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

You will use these CSM 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 CSM 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** command 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 configuration, refer to the *Catalyst 6500 Series Content Switching Module Installation and Configuration Note*.

CSM technical documentation is located online at the following website:

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

Command Modes

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

Note When using the CSM 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 CSM 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 the following:

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

Regular Expressions

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

- match protocol http cookie (cookie map submode), page -24
- match protocol http header (header map submode), page -29
- match protocol http url (URL map submode), page -33

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
“.\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 Commands

This chapter contains an alphabetical listing of the commands necessary to configure the CSM. 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
3.2(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
2.2(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 Cisco Global Site Selector (GSS), 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.

Note When you use the CSM as a CAPP agent, the CSM does not support multiple vservers with the same domain name. You must give a unique domain name to each vserver on the CSM, using the "domain (virtual server submode)" command. In the GSS, the domain names are configured as tag names in the **keepalive type kalap** command.

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
2.2(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
2.2(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
2.2(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 module.
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
3.2(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 software. This process takes about 3 seconds.

The **ft active** command is used to force the active CSM to the failover state. The 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
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
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
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

Command History

Release	Modification
1.1(1)	This command was introduced.

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
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
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
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
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
priority (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.
mode {**all** | **any**}	Configures tracking mode for all devices or any device.

Defaults

This command has no default settings.

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

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
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

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

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

Defaults

Value is 10.

Command Modes

SLB fault-tolerant configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
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

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 c**ommand 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
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 the **hw-module csm standby config-sync** 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, other than those necessary for communication between the active and standby CSMs, from the fault-tolerant VLAN.

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.

Note This command requires Cisco IOS release 12.2(18)SXD or later in the MSFC.

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
priority (fault tolerant submode)
ip address (VLAN 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
1.1(1)	This command was introduced.
2.1(1)	This command now enables **module csm** commands for the **rp** mode.

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
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
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
3.1(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
1.1(1)	This command was introduced.
4.1(1)	HTTP method parsing support 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
2.1(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
3.1(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 specify each special parameter only 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
2.1(1)	This command was introduced.

Usage Guidelines

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

Header regular expressions (see the "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 provided that 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
2.2(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
2.2(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
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 *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
1.1(1)	This command was introduced.
4.1(1)	HTTP method parsing support 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
2.1(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** 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
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 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
4.1(1)	This command was introduced.
4.2(1)	Increased ROUTE_UNKNOWN_FLOW_PKTS value to 2 for SYN packets. Added the following variables: • MAX_VSERVERS_PER_VIP • MSTS_RDP_VIP_LIST • REAL_SLOW_START_ENABLE • SECURE_HTTP_PRIV_KEY_FILE • SECURE_HTTP_PORT • SECURE_HTTP_SERVER_CERTIFICATE • SECURE_HTTP_SSL_METHOD • SECURE_HTTP_TFTP_HOST_IPADDRESS • SECURE_SASP_ENABLE • SECURE_SASP_SSL_METHOD • SECURE_SASP_TFTP_HOST_IPADDRESS • SECURE_SASP_SERVER_CERTIFICATE • SECURE_SASP_PRIV_KEY_FILE

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_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)
ARP_REPLY_FOR_NO_INSERVICE_VIP	0	Integer (0 to 1)	Specifies whether the CSM replies to ARP for out-of-service virtual server (1)
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 or not 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 characters)	Configures the expiration time and date for the HTTP cookie inserted by the CSM
CSM_FAST_FIN_TIMEOUT	10	Integer (10 to 65535)	Specifies the timeout (in seconds) for connection reset after FIN is detected
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 fault-tolerant 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 characters)	Configures the list of delimiter characters for cookies in the URL string
INFINITE_IDLE_TIME_MAXCONNS	1024	0 to 4294967295	Configures the maximum number of connections that can have infinite idle time

Name	Default	Valid Values	Description
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 virtual servers that can have the same IP address—values are specified as powers of 2 (for example, 2^7=128, 2^10=1024)
MSTS_RDP_VIP_LIST	none	String (up to 256 bytes)	Configures a list of virtual servers that support Microsoft Terminal Services Remote Desktop Protocol (MSTS-RDP)
NAT_CLIENT_HASH_SOURCE_PORT	0	Integer (0 to 1)	Specifies whether to use the source port to pick the client NAT IP address
NO_RESET_UNIDIRECTIONAL_FLOWS	0	Integer (0 to 1)	Specifies, if set, that unidirectional flows do not be reset when timed out
REAL_SLOW_START_ENABLE	3	Integer (0 to 10)	Disables or enables the slow start feature with the average number of connections sent to the slowstart server. The values are specified as powers of 2
ROUTE_UNKNOWN_FLOW_PKTS	0	Integer (0 to 3)	For packets that do not match any existing flows, specifies whether to not route SYN or non-SYN packets (0), route non-SYN packets (1), route SYN packets (2), or route SYN and non-SYN packets (3).
SECURE_HTTP_PRIV_KEY_FILE	none	String (0 to 256 characters)	Specifies the private key file used by the HTTPS server
SECURE_HTTP_PORT	443	Integer (1 to 65535)	Specifies the HTTPS server port number
SECURE_HTTP_SERVER_CERTIFICATE	none	String (0 to 256 characters)	Specifies the certificate file used by the HTTPS server
SECURE_HTTP_SSL_METHOD	0	Integer (0 to 3)	Specifies the SSL version used by the HTTPS server
SECURE_HTTP_TFTP_HOST_IPADDRESS	none	String (0 to 16 characters)	Specifies the IP address of the TFTP server that contains the HTTP server certificates. If this variable is not set, the MSFC becomes the default TFTP server and the CSM implicitly looks for the certificates on the MSFC filesystems.
SECURE_SASP_ENABLE	0	Integer (0 to 1)	Specifies whether Secure SASP feature is enabled (1)

Name	Default	Valid Values	Description
SECURE_SASP_SSL_METHOD	0	Integer (0 to 3	Specifies the SSL version used by the SASP Client
SECURE_SASP_TFTP_HOST_IPADDRESS	none	String (0 to 16 characters)	Specifies the IP address of the TFTP server that contains the SASP client certificates. When this variable is not set, the MSFC becomes the default TFTP server andthe CSM implicitly looks for the certificates on the MSFC filesystems
SECURE_SASP_SERVER_CERTIFICATE	none	String (0 to 256 characters)	Specifies the certificate file used by the Secure SASP client
SECURE_SASP_PRIV_KEY_FILE	none	String (0 to 256 characters)	Specifies the private key file used by the Secure SASP client
SWITCHOVER_RP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine route processor switchover occurs
SWITCHOVER_SP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine switch processor 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 characters)	If “true,” responds to ICMP probes regardless of virtual server state
XML_CONFIG_AUTH_TYPE	Basic	String (5 to 6 characters)	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
4.1(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
3.1(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
3.1(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
3.1(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
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 (virtual server submode)

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
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.

The CSM supports only contiguous bits in the definition of the wildcard in the **ip access-list** command. Therefore, a valid wildcard contains a set of zeros followed by a set of ones.

For example, wildcard 0.0.255.255 corresponds to a subnet mask of 255.255.0.0. Wildcard 0.0.255.254 also corresponds to a subnet mask of 255.255.0.0 (the non-contiguous zero in the last bit of the wildcard is ignored).

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
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
2.1(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 on page A-18.

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
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 outservice** *real_value* [sticky] **inservice** *real_value*[**sticky**]]]

no serverfarm

Syntax Description

primary-serverfarm	Character string used to identify the server farm.
backup *sorry-serverfarm*	(Optional) Sets the sorry-serverfarm name to the backup server farm.
sticky	(Optional) Enables stickiness to the backup server.
threshold	(Optional) Configures the serverfarm health threshold.
inservice *real_value*	(Optional) Specifies the number of active real servers required for the serverfarm 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
1.1(1)	This command was introduced.
3.1(1)	The sorry server (backup server) option was added to this command.
4.2(1)	The **threshold outservice** *real_value* **inservice** *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 packet, 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
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
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
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
1.1(1)	This command was introduced.

Usage Guidelines

A probe can be assigned to a server farm in serverfarm submode, or to a real server in real server 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
```

Use the **health probe** command in the SLB real server configuration submode to apply a probe to a specific real server. Use the **probe** command in the SLB serverfarm configuration submode to apply a probe to all servers in a server farm.

Examples

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

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

Related Commands

health probe (real server submode)
probe (serverfarm submode)
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
2.1(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
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 serverfarm, 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.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
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
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, as shown in this example:

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

`expect status 0 4` 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
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
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
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
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
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
3.1(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
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
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 3
```

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
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
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
	3.1(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
recover (probe submode)
retries (probe submode)
script file
show module csm probe

real

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

real {*ip-address* [*port*] | *real_name*[*port*]}

no real {*ip-address* [*port*] | *real_name* [*port*]}

Syntax Description

ip-address	Real server IP address.
real_name	Character string used to identify the real server; the character string is limited to 15 characters.
port	(Optional) Port translation for the real server; the range is from 1 to 65535.

Defaults

The default is no port translation for the real server.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The ability to define *real_name* 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.

After creating a real server at the CSM module level, you can assign the real server to a server farm using the **real** command in the SLB serverfarm configuration submode.

Usage Guidelines

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 by 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**—Using the **inservice standby** command in the real server submode, the CSM is specified as standby. Sticky is allowed, but no new connections are allowed.

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

address (real server submode)

When you define a real server by a name rather than an IP address, use the **address** command in the SLB real server configuration submode to assign an IP address .To remove the address from the configuration, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	Real server IP address.

Defaults

This command has no default settings.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced with the real_name feature.

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.

Examples

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

```
Cat6k-2(config-slb-real)# address 130.21.34.56
```

Related Commands

real
show module csm real

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 arguments or keywords.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
3.2(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
1.1(1)	This command was introduced.

Usage Guidelines

Define the probe and configure its behavior using the CSM module-level **probe** command.

The **health probe** command applies the probe to a single real server. To apply a probe to all real servers in a server farm, use the **probe** command in the serverfarm submode.

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

probe
probe (serverfarm submode)
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 default is that a real server is not in service.

Command Modes

SLB real server configuration submode

Command History

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

Usage Guidelines

The **standby** keyword is used to remove a real server from rotation when you want to allow sticky and existing connections to continue. You can then set the real server to **no inservice** to remove the remaining active connections.

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 after 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.

When you have created a module-level real server by a name rather than an IP address, the **no inservice** command will affect all server farm real servers with the same name.

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

location (real server submode)

Using the **location** command in the SLB real server configuration submode, you can store an opaque string that will be printed when the real server is displayed. To remove the address from the configuration, use the **no** form of this command.

location *location-string*

no location *location-string*

Syntax Description

location-string	An opaque string that is printed when the real is displayed.

Defaults

This command has no default settings.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced with the real_name feature.

Usage Guidelines

As a means to track where a real server is located, this command accepts a string that is printed when the real server is displayed. You can use the location string to filter the output of the **show module csm <slot> real** command.

Examples

This example shows how to configure a location description for the real server:

```
Cat6k-2(config-slb-real)# location SantaClara
```

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
1.1(1)	This command was introduced.

Usage Guidelines

When you specify the **minconns** command, you must also specify the **maxconns** command.

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 minimum number of connections.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
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.

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
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
1.1(1)	This command was introduced.

Usage Guidelines

When the server farm's load-balancing predictor algorithm is round-robin or leastconns, a real server whose weight is twice that of another will receive approximately twice the connections of the lower weighted server.

The server weights are relative; is not necessary that the weights add to 100.

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
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
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

show module csm vserver redirect
virtual (virtual server submode)

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
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

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

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
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
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

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
2.1(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
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
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
2.1(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

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

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
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
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
1.1(1)	This command was introduced.
3.1(1)	The **IP reverse-sticky** command is 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

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

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 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
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
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
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
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.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
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	Specifies 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
3.2(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
2.2(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
1.1(1)	This command was introduced.
3.2(1)	This command was modified to include the **static** option.

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

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*] **static**

no nat server

Syntax Description

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

Defaults

Server NAT is enabled by default.

Command Modes

SLB server farm configuration submode

Command History

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

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, and 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
1.1(1)	This command was introduced.
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.
4.1(2)	The REAL_SLOW_START_ENABLE variable was included to control the rate at which a real server ramps up and is put into service.
4.2(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 serverfarm 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 serverfarm.

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 p1_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
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

real (serverfarm submode)

To configure a real server to be a member of the server farm, first create and configure the real server using the CSM module-level **real** command. To add the real server to a 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*]

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.

Defaults

The default is no port translation for the real server.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Usage Guidelines

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 by 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**—Using the **inservice standby** command in the real server submode, the CSM is specified as standby. Sticky is allowed, but no new connections are allowed.

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

real name (serverfarm submode)

To configure a named real server to be a member of the server farm, create and configure the real server using the CSM module-level **real** command. To add the real server to a server farm, use the **real name** command in the SLB serverfarm configuration submode. To remove the real server from the serverfarm, use the **no** form of this command.

real name *real_name* [*port*]

no real name *real_name* [*port*]

Syntax Description

real_name	Character string used to identify the real server; the character string is limited to 15 characters.
port	(Optional) Port translation for the real server; the range is from 1 to 65535.

Defaults

The default is no port translation for the real server.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The IP address and other settings are configured using the module-level **real *name*** command. In the real name configuration submode, the same commands are available as in the real *ip-address* configuration submode.

Usage Guidelines

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 by 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**—Using the **inservice standby** command in the real server submode, the CSM is specified as standby. Sticky is allowed, but no new connections are allowed.

Examples

This example shows how to add a named real server and enter the real name server submode:

```
Cat6k-2(config-slb-sfarm)# real name EXAMPLE
Cat6k-2(config-slb-real)#
```

Related Commands

inservice (real server submode)
real
script task
show module csm real
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
2.2(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
3.2(1)	This command was introduced as **show ip slb**.

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

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
2.2(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
1.1(1)	This command was introduced as **show ip slb conns**.
2.1(1)	This command was changed to **show module csm** *slot (for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb dfp**.
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)*.

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

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
1.1(1)	This command was introduced as **show ip slb map**.
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.
2.2(1)	This command was changed to include the **retcode** option.

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 virtual server memory information in detail.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb memory**.
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.

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
1.1(1)	This command was introduced as **show ip slb natpool**.
2.1(1)	This command was changed to **show module csm** *slot* **natpool** *(for* **ip slb mode rp** *only)*.

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
3.1(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
1.1(1)	This command was introduced as **show ip slb policy**.
2.1(1)	This command was changed to **show module csm** *slot* **policy** *(for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb probe**.
2.1(1)	This command was changed to **show module csm** *slot* **probe** *(for* **ip slb mode rp** *only)*.

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
3.1(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
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**] [**location** *string*]

Syntax Description

slot	Slot where the CSM resides.
sfarm	(Optional) Displays real servers for only a single serverfarm.
sfarm-name	(Optional) Name of the server farm to restrict output.
detail	(Optional) Displays detailed information.
location	(Optional) Displays only real servers whose location strings match.
string	(Optional) Location string to restrict output.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb real**.
2.1(1)	This command was changed to **show module csm** *slot* **real** *(for* **ip slb mode rp** *only)*.
3.1(1)	This command was changed to allow restricting output based on location string.

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 dynamically 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 currently open.
remaining retries	Number of retries remaining showing the inband health of a real server.
minconns	Minimum connections configured to the real server. maxconns If minconns and maxconns are changed from their default values, they enable the connection watermarks feature. No more than the maxconns connections are active on this real server. When the server has reached its maximum, the CSM stops sending new connections until the number of active connections drops below the minconns value.
maxconns	Maximum connections configured to the real server.
weight(admin)	Weight you configured and assigned to the real server which identifies the capacity of the real server compared to other real servers in the server farm. **Note** When using DFP (Dynamic Feedback Protocol), then the dynamic weight can be different from the admin weight.
metric	Health metric sent to the DFP manager.
remainder	Remaining number of connections.
total conns established	Total connections that have been set up since the last reset of the counters with the **clear mod csm 6 counters** command.
total conn failures	Total connections that have failed.

Related Commands

module csm
real (static NAT submode)
location (real server 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** *sfarm-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
2.2.1	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
3.1(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 task

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
3.1(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
1.1(1)	This command was introduced as **show ip slb serverfarm**.
2.1(1)	This command was changed to **show module csm** *slot* **serverfarm** *(for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb static**.
2.1(1)	This command was changed to **show module csm** *slot* **static** *(for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb static server**.
2.1(1)	This command was changed to **show module csm** *slot* **static server** *(for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb stats**.
2.1(1)	This command was changed to **show module csm** *slot* **stats** *(for* **ip slb mode rp** *only)*.

Usage Guidelines

The statistics counters are 32-bit. Totals are accumulated since the last time the counters were cleared.

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 on the CSM.
Connections Destroyed	Number of connections that have been destroyed on the CSM.
Connections Current	Number of current connections at the time the command was issued.
Connections Timed-Out	Number of connections that have timed out, which can occur for the following reasons: • connection has been idle (in one or both directions) for longer than the configured idle timeout. • TCP connection setup not completed successfully.
Connections Failed	Number of connections failed because the server did not respond within the timeout period, or the server replied with a reset.
Server initiated Connections	Number of connections created by real servers, the number of current connections, and the number of connections that failed (because the destination is unreachable).
L4 Load-Balanced Decisions	Number of Layer 4 load-balancing decisions attempted.
L4 Rejected Connections	Number of Layer 4 connections rejected because no real server was available
L7 Load-Balanced Decisions	Number of Layer 7 load-balancing decisions attempted.
L7 Rejected Connections: Total	Number of Layer 7 connections rejected.
L7 Rejected Connections: Parser	Number of Layer 7 connections rejected because the Layer 7 processor in the CSM ran out of session buffers to save the parsing state for multi-packet HTTP headers. The **show module csm <x> tech-support proc 3** command will show detailed buffer usage.
L7 Rejected Connections: Reached max parse len	Number of Layer 7 connections rejected because the HTTP header in the packet is longer than **max-parse-len.** When a virtual server is configured with HTTP persistent rebalancing or cookie matching/sticky, the CSM must parse to the end of HTTP header. The default **max-parse-len** value is 2000 bytes.
L7 Rejected Connections: Cookie out of mem:	Number of Layer 7 connections rejected because of no memory to store cookies. When a virtual server is configured with cookie matching, the CSM must save the cookie contents in memory.
L7 Rejected Connections: Cfg version mismatch	Number of Layer 7 connections rejected because part of the request was processed with an older version of the configuration. This counter should only increase after configuration changes.
L7 Rejected Connections: Bad SSL2 format:	Number of Layer 7 connections rejected because the request is using an unsupported SSL format or the format is not valid SSL.

Table 2-3 show module csm stats Command Field Information (continued)

Field	Description
L4/L7 Rejected Connections	Number of Layer 4 and Layer 7 connections rejected for policy related reasons: No policy: connection rejected because the request matched a virtual server, but this virtual server did not have a policy configured. No policy match: connection rejected because the request matched a virtual server, but the request did not match any policy configured on the virtual server. No real: connection rejected because no real server was available to service the request ACL denied: connection rejected because a request matched a policy with a client-access-list entry and the entry is configured to deny the request. Server Initiated: connection initiated by a real server is rejected.
Checksum Failures	Number of checksum failures detected (there are separate counters for IP and TCP failures).
Redirect Connections	Number of connections redirected, and the number of redirect connections dropped.
FTP Connections	Number of FTP connections opened.
MAC Frames	Number of MAC frames received and transmitted on the CSM backplane connection.

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
1.1(1)	This command was introduced as **show ip slb status**.
2.1(1)	This command was changed to **show module csm** *slot* **status** (*for* **ip slb mode rp** *only*).

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
1.1(1)	This command was introduced as **show ip slb sticky**.
2.1(1)	This command was changed to **show module csm** *slot* **sticky** *(for* **ip slb mode rp** *only.*

Usage Guidelines

This command displays only 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
3.1(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
1.1(1)	This command was introduced as **show ip slb tech-support**.
2.1(1)	This command was changed to **show module csm** *slot* **tech-support** *(for* **ip slb mode rp** *only)*.

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
3.1(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 the client VLAN configuration only.
server	(Optional) Displays the server VLAN configuration only.
ft	(Optional) Displays the fault-tolerant configuration only.
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
1.1(1)	This command was introduced as **show ip slb vlan**.
2.1(1)	This command was changed to **show module csm** *slot* **vlan** *(for* **ip slb mode rp** *only)*.

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
1.1(1)	This command was introduced as **show ip slb vserver redirect**.
2.1(1)	This command was changed to **show module csm** *slot* **vserver redirect** *(for* **ip slb mode rp** *only)*.

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
3.1(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
3.1(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
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
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
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

static
show module csm 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** *name* [**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 stickiness based on the SSL session ID.
header *name*	Specifies stickiness based on the HTTP header.
address **[source | destination | both]**	(Optional) Specifies stickiness based on the source IP address, the destination IP address, or both addresses.
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
1.1(1)	This command was introduced.
2.1(1)	Changed the default timeout from 0 to 1440.
4.1(1)	The **insert** keyword was added.
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.

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.

Note The configurable timeout values are not applied when using cookie insert. You can adjust the timeout value using the environment variables.

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)#
```

When defining the sticky group use the Router(config-module-csm)# **sticky 5 cookie mycookie insert timeout** *X* command.

When applying the sticky group to a virtual server, use these comands:

```
Router(config-slb-sfarm)# vserver barnett
Router(config-slb-vserver)# virtual 10.1.0.85 tcp 80
Router(config-slb-vserver)# serverfarm bosco
Router(config-slb-vserver)# sticky X group 5
Router(config-slb-vserver)# inservice
```

X=timeout value

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
4.1(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)
sticky
sticky (virtual server submode)
sticky-group (policy submode)
show module csm sticky

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
4.1(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

sticky
sticky (virtual server submode)
sticky-group (policy submode)
show module csm sticky

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
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 the 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
3.2(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

sticky
sticky (virtual server submode)
sticky-group (policy submode)
show module csm sticky

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
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
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
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

client-group (policy submode)
ip access-list standard
show module csm vserver redirect
vserver

description (virtual server submode)

To add a description for the serverfarm, 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.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
4.2(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

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
2.2(1)	This command was introduced.

Usage Guidelines

Use the **domain** command to specify a domain name for the virtual server. The domain name must uniquely identify only one virtual server.

The Cisco Global Site Selector (GSS) sends keepalive queries to a virtual server using the domain name to identify the specified server. In the GSS, the domain name is called the tag name.

Examples

This example shows how to set a domain name:

```
Cat6k-2(config-slb-vserver)# domain cisco.com
```

Related Commands

capp udp
vserver

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
1.1(1)	This command was introduced.
4.2(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

show module csm vserver redirect
vserver

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 default is the virtual server is not in service.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
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

show module csm vserver redirect
vserver

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
3.1(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

vserver

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* | **default-policy**}

no parse-length

Syntax Description

bytes	Number of bytes; the range is from 1 to 4000.
default-policy	Sets the default policy when the maximum parse length is reached for a session.

Defaults

The default is 2000.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
4.2(1)	The **default-static** option 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

show module csm vserver redirect
vserver

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
2.2(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

show module csm vserver redirect
vserver

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
2.1(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

show module csm vserver redirect
vserver

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
2.1(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

ft group
show module csm vserver redirect
vserver

reverse-sticky (virtual server submode)

To ensure that the CSM will switch 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
1.1(1)	This command was introduced.
3.1(1)	The **IP reverse-sticky** command is 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

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

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 serverfarm health threshold.
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.*
inservice *real_value*	(Optional) Specifies the number of active real servers required for the serverfarm to be activated.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The backup server option was added to this command.
4.2(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

serverfarm (policy submode)
show module csm vserver redirect
vserver

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*	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
1.1(1)	This command was introduced.
4.2(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

policy
show module csm owner
show module csm vserver redirect
vserver

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
3.1(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

policy
show module csm owner
show module csm vserver redirect
vserver

status-tracking (virtual server submode)

To link virtual servers to create a virtual server dependency, use the **status-tracking** *vserver_name* 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
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

vserver

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
1.1(1)	This command was introduced.
3.1(1)	The IP reverse-sticky optional parameters are 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 used in this submode must correspond to an existing sticky group created using the **sticky** command in the CSM module-level submode. 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

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

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
2.1(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
1.1(1)	This command was introduced.
2.1(1)	*ip-netmask*, UDP/arbitrary protocol introduced.
2.2.1	RTSP support was introduced.
3.2(1)	Added TCP termination for DoS attack prevention and per packet load balancing.

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).

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

show module csm vserver
vserver

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
2.1(1)	This command was introduced.
3.1(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** or **vserver detail** commands.

As a default, the CSM selects unidirectional for a UDP protocol virtual server.

Note When a virtual server is configured as unidirectional, it no longer uses the pending timer. Instead, the idle timer will determine when to close idle or errant flows. Because the idle timer has a much longer default duration than the pending timer, be sure to set the idle timer to an appropriate value.

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

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*

no vlan

Syntax Description

vlan-number	VLAN that the virtual server may access.

Defaults

The default is all VLANs.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
2.1(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**	Specifies the client-side or server-side VLAN.

Defaults

The default is all VLANs.

Command Modes

SLB configuration submode

Command History

Release	Modification
2.1(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
1.1(1)	This command was introduced for server VLANs.
2.1(1)	This command is now available for both client and server VLANs.

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.

Note If you intend to use RHI, be sure to define an alias IP address.

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.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

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
1.1(1)	This command was introduced for client VLANs.
2.1(1)	This command is now available for both client and server VLANs.

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
1.1(1)	This command was introduced.
2.2.1	Increases maximum number of unique VLAN IP addresses per system form 32 to 255.
4.2(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
1.1(1)	This command was introduced for server VLANs.
2.1(1)	This command is now available for both client and server VLANs.

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
3.1(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
3.1(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
3.1(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
3.1(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
3.1(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
3.1(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)

INDEX

A

active connection
  displaying **2-121**
  limiting **2-82**
address pool
  client **2-35**
Address Resolution Protocol
  See ARP
agent configuration
  CAPP UDP **2-4**
algorithm
  load balancing predictor **2-101, 2-108**
ARP
  cache **2-34, 2-118**
  configuring a static entry **2-2**
associating
  policy attributes **2-45**
attributes
  associating to policy **2-45**
  configuring for virtual server **2-190**
audience **ix**
authentication
  HTTP
    probe **2-58**
    probe credentials **2-57**

B

backup
  string **2-95**
beginning and ending URL **2-189**
billing information
  owner object **2-42**
byte parsing
  URL and cookie **2-177**

C

capacity
  real server **2-85**
CAPP
  configuration and statistics **2-119**
  enter submode **2-3**
Cisco modes **2-21**
client
  address pool **2-35**
  group **2-45**
  group XML **2-202**
  NAT **2-35**
    pool addresses **2-49, 2-106**
  removing definition **2-88**
  restricting for virtual server **2-171**
  sticky connections **2-187**
command modes
  changing **1-2**
  configuration **1-2**
  privileged **1-2**
  unprivileged **1-2**
commands
  abbreviating **1-1**
  changing modes **1-2**
  completing **1-1**
  firewall CLI help **1-1**
connection
  backup real server **2-77**

balancing to server **2-45**
count for owner objects **2-130**
maximum number **2-44**
pending timeout **2-178**
redundancy **2-91**
redundancy for virtual server **2-180**
reverse sticky **2-181**
shutdown **2-77**
content
router **2-3**
switching policy **2-27**
Content Application Peering Protocol
See CAPP
controlling serverfarm start **2-109**
cookie
byte parsing **2-177**
length **2-165**
map **2-45, 2-47**
offset **2-165**
cookie map
map cookie **2-23**
match rules **2-24**
regular expressions **2-24**
credentials
HTTP probe authentication **2-58**
probe authentication **2-57**
XML **2-203**

D

DFP
agent **2-10, 2-123**
agent unique ID **2-102**
external **2-11**
fault-tolerant statistics and counters **2-125**
manager **2-123**
submode **2-9**
differentiated services code point
See DSCP
displaying
active connections **2-121**
ARP cache **2-118**
CAPP configuration and statistics **2-119**
DFP agent and manager information **2-123**
loaded scripts **2-140**
memory use **2-128**
module statistics **2-145**
module status **2-148**
NAT configurations **2-129**
owner object connections **2-130**
policy configurations **2-131**
private VLAN information **2-134**
probe data **2-132**
probe script data **2-133**
real server information **2-135**
return code configuration **2-138**
script contents **2-139**
script status **2-151**
server farm information **2-141**
server NAT configuration **2-117, 2-143**
static server information **2-144**
sticky database **2-149**
technical support information **2-152**
URL map information **2-126**
virtual servers **2-158**
VLAN list **2-157**
XML statistics **2-159**
DNS
domain **2-26**
domain name for probe **2-65**
map **2-25**
probe **2-56**
probe optional port **2-67**
regular expressions **2-25**
documentation
conventions **x**
organization **ix**
domain

DNS **2-25**
name for DNS probe **2-65**
name setting **2-173**
Domain Name System
See DNS
DSCP
value **2-52**
Dynamic Feedback Protocol
See DFP

E

enabling
XML **2-201, 2-206**
encryption
inbound CAPP datagrams **2-7**
packet encryption **2-5**
environmental variables **2-36, 2-155**
exit
see logging out **2-12**
extensible markup language
See XML
external DFP manager **2-11**

F

failed
probe retries **2-71**
server behavior **2-104**
server probe **2-62**
failover **2-15**
fault tolerance **2-13**
fault-tolerant
pair **2-125**
traps **2-160**
fields
insert header **2-28**
File Transfer Protocol
See FTP
FTP
probe **2-60**

G

gateway
VLAN IP address **2-198**
global security **2-5**
group
fault-tolerant **2-13**
GSLB
probes **2-56**

H

hash
ULR patterns **2-189**
header
field for probe **2-63**
header fields
specifying **2-29**
header map
match rules **2-29**
regular expression **2-29**
specifying **2-48**
health
IP address for ICMP **2-57**
monitoring
by configuring probes **2-55**
using script files **2-98**
real server retries **2-105**
heartbeat
interval **2-16**
messages **2-13, 2-15**
transmissions **2-16**
host **2-29**
route designation for redirect virtual server **2-87**

host route
virtual server **2-170**
HTTP
backup request **2-95**
header expression group **2-48**
header field insert **2-28**
header group **2-27**
headers **2-27**
probe **2-56, 2-60, 2-70**
authentication **2-58**
header field **2-63**
probe authentication **2-57**
regular expressions **2-28, 2-29**
relocation string **2-96**
Hypertext Transfer Protocol
See HTTP

I

ICMP
IP address **2-57**
probe **2-56**
identifying
virtual server **2-169**
idle timer **2-89**
insert header fields **2-28**
inserting header fields **2-28**
Internet Control Message Protocol
See ICMP
Internet Protocol
See IP
interval
between probes **2-63**
IP
address
advertisement **2-87**
for probe on VLAN **2-199**
assigning multiple **2-195**

K

KAL-AP
probe **2-56**
keepalive messages **2-10**

L

least connections
slow start **2-109**
leaving submodes **2-12**
length
cookie **2-165**
load balancing **2-34**
algorithm (predictor) **2-101**
device **2-21**
enabling a virtual server **2-175**
policy **2-184**
target **2-73, 2-76, 2-112**
URL hash **2-189**
loaded scripts **2-140**
logging out **2-12**

M

map
HTTP header **2-27**
match rules
cookie maps **2-23, 2-24**
header map **2-29**
MD5
authentication **2-5**
hashing **2-5**
memory
use **2-128**
migrating
configurations **2-34**
modes
Cisco IOS SLB **2-21**

command **1-2**
module
status **2-148**
multiple
assigning IP addresses **2-195**
match rules for URL maps **2-33**
module configuration **2-34**
probes **2-111**

N

NAT
client **2-35, 2-49, 2-106**
configuration **2-129**
pool addresses **2-35, 2-49, 2-106**
real server **2-162**
specifying to servers **2-107**
network
configuring routes **2-200**
Network Address Translation
See NAT

O

offset
cookie **2-165**
optional port
DNS probe **2-67**
owner
billing information **2-42**
configuring maximum number of connections **2-44**
contact information **2-42, 2-43**
object **2-41**
virtual server **2-176**

P

pending connection timeout **2-178**
persistence
cookie offset and length **2-165**
persistent
rebalance **2-179**
policy
access-list standard **2-46**
client-group **2-46**
configuring **2-45, 2-131**
cookie-map **2-47**
load balancing **2-184**
match DSCP value **2-52**
server farm **2-50**
specifying header map **2-48**
sticky-group **2-53**
url-map **2-54**
pool
NAT **2-35**
predefined HTTP header fields **2-29**
predictor
load balancing algorithm **2-101, 2-108**
preempt
default value **2-17**
priority
default value **2-19**
private VLAN
information **2-134**
probe
credentials **2-58**
data **2-132**
DNS
domain name **2-65**
optional port **2-67**
failed **2-62**
frequency **2-56**
GSLB **2-56**
HTTP
authentication **2-57, 2-58**
header field **2-63**
interval **2-63**

request method for HTTP **2-70**
retries **2-56, 2-71**
script **2-72, 2-98**
data **2-133**
server farm **2-111**
server reply time **2-68**
status code **2-60**
timeout values **2-68**
type **2-55**
VLAN IP address **2-199**
purged connections
server farm **2-104**

R

real server
backup **2-77**
enabling **2-79, 2-84**
health **2-105**
identifying **2-73, 2-112, 2-114**
information **2-135**
maximum connections **2-82**
minimum connection threshold **2-83**
module-level **2-112, 2-114**
placing in service **2-90**
probe configuration **2-78**
redirect virtual server **2-84**
static NAT **2-162**
weight **2-85**
redirect
real server in service **2-90**
traffic from virtual server **2-84**
traffic to server farm **2-86**
virtual server source VLAN **2-94**
virtual server SSL **2-92**
redirect virtual server
IP address advertisement **2-87**
redundancy
connection for redirect virtual server **2-91**
regular expressions
for cookies **2-24**
header map **2-29**
URL **2-33**
related documentation **xi**
restricting clients
redirect virtual server **2-88**
retries
failed probes **2-71**
real server health **2-105**
return code
checking **2-30**
configuration **2-138**
thresholds **2-31**
return code map
server farm **2-116**
reverse sticky
connections **2-181**
removing from policy **2-53**
reverse-sticky **2-97**
route
VLAN **2-200**

S

script
contents **2-139**
data **2-133**
file **2-98**
probe **2-72**
status display **2-151**
task **2-100**
tasks **2-140**
server
identifying a real server **2-73, 2-112, 2-114**
reply
time **2-68**
server farm **2-141**
failed connection purge **2-104**

identification **2-101**
specifying NAT to a server **2-107**
virtual server **2-182**
serverfarm
slow start ramp up **2-109**
Server Load Balancing
See SLB
servers
connection balancing **2-45**
failed **2-62, 2-71**
failed connection behavior **2-104**
NAT **2-107**
behavior **2-161**
configuration **2-117, 2-143**
static **2-144**
session options **2-5**
shutdown
connection to real server **2-77**
single module configuration **2-34**
SLB **2-21**
slow start
serverfarm **2-109**
SMTP
probe **2-60**
source VLAN
accessing virtual server **2-194**
defining **2-193**
redirect virtual server **2-94**
SSL
redirect virtual server **2-92**
sticky operation **2-185**
standalone
script task **2-100**
starting serverfarms
slow start **2-109**
static **2-161**
ARP **2-2**
servers **2-144**
statistics
displaying **2-145**
status code
probe **2-60**
sticky
database display **2-149**
group **2-45, 2-53, 2-97, 2-163**
reverse **2-97, 2-181**
SSL **2-185**
static **2-166, 2-168**
virtual server client connections **2-187**
submodes
leaving **2-12**
syslog messages
return codes **2-31**

T

task
standalone script **2-100**
TCP
connection wait **2-66**
port for XML **2-205**
technical support information
displaying **2-152**
Telnet
probe **2-60**
time
TCP connection wait **2-66**
wait for server reply **2-68**
timeout
pending connection **2-178**
values for probe types **2-68**
timer
idle for redirect virtual server **2-89**
traffic
redirection **2-84, 2-86**

U

UDP
- port **2-56**
- User Datagram Protocol **2-3**

URL
- byte parsing **2-177**
- configuring maps **2-32**
- displaying maps **2-126**
- hashing **2-189**
- multiple match rules **2-33**
- policy maps **2-45**
- regular expressions **2-33**
- removing maps **2-54**

User Datagram Protocol
- see UDP **2-3**

V

values
- DSCP **2-45**

variable
- environmental **2-36, 2-155**

virtual Local Area Network
- *See* VLAN

virtual server
- attributes **2-190**
- connection redundancy **2-180**
- displaying **2-158**
- enabling for load balancing **2-175**
- identifying **2-169**
- idle time **2-174**
- IP address **2-87, 2-93, 2-170**
- owner **2-176**
- persistent rebalance **2-179**
- policy association **2-45**
- redirect **2-84**
- redirected traffic **2-86**
- restricting clients **2-171**
- server farm **2-182**
- setting the domain name **2-173**
- source VLAN **2-193, 2-194**
- sticky **2-187**

VLAN
- alias **2-195**
- configuring routes **2-200**
- gateway IP address **2-198**
- listing **2-157**
- probe IP address **2-199**
- source for redirect virtual server **2-94**
- specifying for XML **2-206**
- virtual server source **2-193, 2-194**

W

webhost
- backup **2-95**
- relocation **2-96**

weight
- real server capacity **2-85**

X

XML **2-204**
- client group address **2-202**
- credentials **2-203**
- enabling **2-201**
- port **2-205**
- statistics display **2-159**
- VLAN **2-206**